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

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

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

**CTL** model checking problem:
- solvable in polynomial time (even PTIME-complete)
  \[ \mathcal{O}(\text{size}(T) \cdot |\Phi|) \]
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
  \[ \mathcal{O}(\text{size}(T) \cdot \exp(|\varphi|)) \]
- **LTL** with fairness:
  \[ \mathcal{O}(\text{size}(T) \cdot \exp(|\varphi| + |\text{fair}|)) \]

---

**CTL** model checking problem:
- solvable in polynomial time (even PTIME-complete)
  \[ \mathcal{O}(\text{size}(T) \cdot |\Phi|) \]
- **CTL** with fairness:
  \[ \mathcal{O}(\text{size}(T) \cdot |\Phi| \cdot |\text{fair}|) \]
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 $\square\Diamond\phi$
- strong fairness $\square\Diamond\psi \rightarrow \square\Diamond\phi$
- weak fairness $\Diamond\Box\psi \rightarrow \square\Diamond\phi$

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 \( \models \)

\[ T \models_{\text{fair}} \varphi \text{ iff } \pi \models \varphi \text{ for all fair paths } \pi \text{ in } T \]
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 \( \Diamond \Box \psi \rightarrow \square \Diamond \phi \)

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

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

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

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 \( \Box \Diamond \phi \)
- 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 \( \models \text{fair} \rightarrow \models \), 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  \( \Box \Diamond \phi \)
- strong fairness  \( \Box \Diamond \psi \rightarrow \Box \Diamond \phi \)
- weak fairness  \( \Diamond \Box \psi \rightarrow \Box \Diamond \phi \)

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

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

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

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

\[ \pi \models \text{fair} \rightarrow \varphi \quad \equiv \quad \Diamond \Box \neg a \lor \varphi \]
CTL fairness assumptions
conjunctions of “formulas” of the type

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

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

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

where \(\psi, \phi\) are CTL state formulas

**note:** CTL fairness assumptions

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

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

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

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

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

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

ctlfair4.4-3
Satisfaction relation for CTL with fairness

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

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

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

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

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

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

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

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

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

\[
\begin{align*}
S & \models_{\text{fair}} \text{true} \\
S & \models_{\text{fair}} a \quad \text{iff} \quad a \in \mathcal{L}(s) \\
S & \models_{\text{fair}} \neg \phi \quad \text{iff} \quad S \not\models_{\text{fair}} \phi \\
S & \models_{\text{fair}} \phi_1 \land \phi_2 \quad \text{iff} \quad S \models_{\text{fair}} \phi_1 \text{ and } S \models_{\text{fair}} \phi_2 \\
S & \models_{\text{fair}} \exists \varphi \quad \text{iff} \quad \exists \pi \in \text{Paths}(s) \text{ with } \pi \models_{\text{fair}} \varphi \\
S & \models_{\text{fair}} \forall \varphi \quad \text{iff} \quad \forall \pi \in \text{Paths}(s): \pi \models_{\text{fair}} \varphi \text{ implies } \pi \models_{\text{fair}} \varphi
\end{align*}
\]
Satisfaction relation for CTL with fairness

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

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

CTL formula

$$\Phi = \forall \square \forall \Diamond start$$
Simple communication protocol

CTL formula:

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

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

\[ \Phi = \forall \square \forall \Diamond \text{start} \]
\[ T \not \models \Phi \]
\[ T \models_{ufair} \Phi \]
\[ T \models_{sfair} \Phi \]

unconditional CTL fairness assumption:

\[ ufair = \square \Diamond \text{delivered} \]

strong CTL fairness assumption:

\[ sfair = \square \Diamond \text{try_to_send} \rightarrow \square \Diamond \text{delivered} \]
Simple communication protocol

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

\[
\Phi = \forall \Box \forall \Diamond start \\
\mathcal{T} \models_{ufair} \Phi \\
?
\]
Simple communication protocol

unconditional fairness: \( ufair = \square \Diamond \exists \bigcirc start \)
Simple communication protocol

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

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

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

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

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

\[
ufair \equiv \Box \Diamond delivered
\]
Simple communication protocol

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

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

\[
\begin{align*}
\Phi &= \forall \Box \forall \Diamond start \\
\mathcal{T} \models_{ufair} \Phi & \checkmark \\
\mathcal{T} \models_{wfair} \Phi & ?
\end{align*}
\]
Simple communication protocol

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

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

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

unconditional fairness: \( ufair = \square \diamond \exists \diamond \text{start} \)

weak fairness: \( wfair = \diamond \square \exists \diamond \text{delivered} \rightarrow \square \diamond \text{delivered} \)

\[ \Phi = \forall \square \forall \diamond \text{start} \]

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

\[ T \models_{wfair} \Phi \quad \text{?} \]

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

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

\[ \Phi = \forall \Box \forall \Diamond start \]
\[ \mathcal{T} \models_{\text{ufair}} \Phi \quad \checkmark \]
\[ \mathcal{T} \models_{\text{wfair}} \Phi \quad \text{wrong} \]

unconditional fairness: \[ \text{ufair} = \Box \Diamond \exists \Box start \]
weak fairness: \[ \text{wfair} = \Diamond \Box \exists \Box \text{delivered} \rightarrow \Box \Diamond \text{delivered} \]

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

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

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

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

\[
\begin{align*}
\Phi & = \forall \Box \forall \Diamond start \\
\mathcal{T} & \models_{ufair} \Phi \quad \checkmark \\
\mathcal{T} & \not\models_{wfair} \Phi \\
\mathcal{T} & \models_{sfair} \Phi \quad ?
\end{align*}
\]
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: \( ufair = \Box \Diamond \exists \Diamond \text{start} \)

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

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

\[ \text{Sat}(\exists \Diamond \text{delivered}) = \{ \text{try_to_send} \} \]
Simple communication protocol

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

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

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

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

\( sfair \equiv \Box \Diamond try\_to\_send \rightarrow \Box \Diamond delivered \)
Simple communication protocol

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

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

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

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

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

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

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

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

\[ sfair \equiv \Box \Diamond \text{try_to_send} \rightarrow \Box \Diamond \text{delivered} \]
If $s \models \forall a \Diamond a$ where $a \in AP$ then $s \models_{fair} \forall a \Diamond a$
Correct or wrong?

\[
\text{If } s \models \forall \diamond a \text{ where } a \in AP \text{ then } s \models^{\text{fair}} \forall \diamond a
\]

correct.
Correct or wrong?

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

correct. Note that:

$s \models \forall \varphi \quad \Rightarrow \quad \text{for all } \pi \in \text{Paths}(s): \quad \pi \models \varphi$
Correct or wrong?

If \( s \models \forall a \diamond \varphi \) where \( a \in AP \) then \( s \models_{\text{fair}} \forall a \diamond \varphi \)

correct.  Note that:

\[
\begin{align*}
  s \models \forall \varphi & \quad \Rightarrow \quad \text{for all } \pi \in \text{Paths}(s) : \pi \models \varphi \\
  & \Rightarrow \quad \text{for all } \pi \in \text{Paths}(s) : \pi \models_{\text{fair}} \varphi \text{ implies } \pi \models \varphi
\end{align*}
\]
If $s \models \forall \diamond a$ where $a \in AP$ then $s \models_{\text{fair}} \forall \diamond a$

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 $\pi \models \varphi$

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

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

correct.

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

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

correct.

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

wrong

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

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

correct.

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

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

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

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

just one fair path ••••••••••••••
Correct or wrong?

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

**Correct.**

If \( s \models \exists \Diamond a \) where \( a \in AP \) then \( s \models_{\text{fair}} \exists \Diamond a \)

**Wrong**

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

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

\[
s \models \exists \Diamond a
\]

just one fair path

\[
\text{just one fair path} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \ldots
\]
Correct or wrong?

If \( s \models \forall \Box a \) where \( a \in AP \) then \( s \models_{\text{fair}} \forall \Box a \)

correct.

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

If \( s \models \forall \Diamond E \Box a \) then \( s \models_{\text{fair}} \forall \Diamond E \Box a \)
Correct or wrong?

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

 wrong

$S_0 \xrightarrow{} S_1 \xrightarrow{} S_2$

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

$\text{green} = \{b\}$
Correct or wrong?

If \( s \models \forall \Box \exists \Box a \) then \( s \models^{\text{fair}} \forall \Box \exists \Box a \)

wrong

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

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

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

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

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

Wrong

\[
\begin{align*}
\text{false} & = \{ b \} \\
\text{true} & = \{ a \}
\end{align*}
\]

\[
\begin{align*}
\text{fair} & = \Box \Diamond b \\
\text{Sat}(\exists \Box a) & = \{ s_0, s_1 \} \\
\text{Sat}(\forall \Diamond \exists \Box a) & = \{ s_0, s_1 \}
\end{align*}
\]
Correct or wrong?

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

wrong

$s_0$

$s_1$

$s_2$

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

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

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

$fair = \Box \Diamond b$

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

$\textcolor{green}{\equiv} = \{b\}$
Correct or wrong?

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

**Wrong**

```
Sat(\exists \Box a) = \{s_0, s_1\}
Sat_{fair}(\exists \Box a) = \emptyset
Sat(\forall \Diamond \exists \Box a) = \{s_0, s_1\}
Sat_{fair}(\forall \Diamond \exists \Box a) = \emptyset
```

**fair = \Box \Diamond b**

```
\emptyset = \{b\}
\{a\} = \{a\}
```
\( \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = ? \)
$\text{Sat}_{\text{fair}}(\exists \Box \text{true}) = \ ?$

CTLFAIR4.4-11

- $\circ = \{a\}$
- $\bullet = \emptyset$

\[\text{fair} = \Box\Diamond a\]
\[ \text{Sat}_{\text{fair}}(\exists \Box \text{true}) = ? \]

CTLFAIR4.4-11

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

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

\[
\text{Sat}_{\text{fair}}(\exists \lozenge \text{true}) = \{s_0, s_2\}
\]

\( \text{fair} = \Box \Diamond a \)

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

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

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

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

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

$公平 = \Box \Diamond a$

$= \{a\}$

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

**CTLFAIR4.4-11**

- Red node: \(= \{a\}\)
- Blue node: \(= \emptyset\)
- \(fair = \Box \Diamond a\)

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

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

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

**fair** is realizable iff

\(Sat_{\text{fair}}(\exists \square \text{true}) \supseteq\) set of all reachable states
Model checking problem for FairCTL
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 $\mathcal{T}$
CTL formula $\Phi$
CTL fairness assumption $\textit{fair}$, e.g.,

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

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

given:
- finite transition system \( \mathcal{T} \)
- CTL formula \( \Phi \)
- CTL fairness assumption \( \text{fair} \), e.g.,

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

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

\[ \exists \bigcirc, \exists \bigvee, \exists \bigodot \]
Preprocessing of FairCTL model checking

**given:** finite transition system $T$

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 $T \models_{fair} \Phi$ hold?
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.,

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

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

preprocessing: apply a standard CTL model checker to evaluate the CTL state subformulas of $\text{fair}$
**Preprocessing of FairCTL model checking**

*given:* finite transition system $T$

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

CTL fairness assumption $\text{fair}$, e.g.,

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

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

*preprocessing:* apply a standard CTL model checker to evaluate the CTL state subformulas of $\text{fair}$

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

given: finite transition system $T$

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

CTL fairness assumption $\textit{fair}$, e.g.,

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

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

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

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

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

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

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 $\mathcal{T}$

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

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

1. ... preprocessing ...
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 $fair$

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:
   - $true$, $a \in AP$, $\land$, $\lnot$: as for standard CTL
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
Idea of FairCTL model checking

given: finite transition system $T$

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

CTL fairness assumption $\textit{fair}$

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

1. ... preprocessing ... 

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

   - $\textit{true}$, $a \in AP$, $\land$, $\neg$: as for standard CTL
   - $\exists \Box$, $\exists U$: via standard CTL model checking
   - $\exists \Box$: 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:

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

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

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

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

\[
\begin{align*}
\text{fair} &= \square \lozenge \text{red} \\
\models_{\text{fair}} s' \not= \exists \bigcirc \text{green}
\end{align*}
\]
FairCTL model checking: treatment of $\exists \bigcirc$

Fair $= \Box \Diamond red$

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

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

introduce an additional atomic proposition $a_{\text{fair}}$

s.t. for all states $s$:

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

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

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

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

\[\begin{align*}
    fair &= \square \Diamond red \\
    s &\not\models_{\text{fair}} \exists\bigcirc \text{green} \\
    \text{as } s' &\not\models_{\text{fair}} \exists\square \text{true}
\end{align*}\]

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

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

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 $s$:

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

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

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

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

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

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

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

\[
\begin{align*}
    s \models_{\text{fair}} \exists\Box b & \iff s \models \exists\Box (b \land a_{\text{fair}}) \\
    s \models_{\text{fair}} \exists(c \cup b) & \iff s \models \exists(c \cup (b \land a_{\text{fair}}))
\end{align*}
\]
FairCTL model checking: $\exists \Box$ and $\exists U$

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

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

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

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

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

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

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

$\mathcal{T}$

$\{b\}$

$\{c\}$

$\emptyset$

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

CTL formula $\exists \Diamond c$

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

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

$$\mathcal{T}$$

$$\{b\}$$

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

$$\mathcal{T}$$

$$\{b\}$$

CTL formula $\exists \diamond c$

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

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

CTL formula $\exists \Diamond c$

$\models (c \land a_{\text{fair}})$

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

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

CTL formula $\exists \diamond c$

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 $\exists U$

$\mathcal{T}$:

$\emptyset$

$\{c\}$

$\{b\}$

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

$\mathcal{T}$:

$\begin{align*}
\mathcal{T} & : s \\
& \xrightarrow{} \emptyset \\
& \xrightarrow{} \{c\} \\
& \xrightarrow{} \{b\}
\end{align*}$

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

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

$\mathcal{T}$:

$\exists$ untreated

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

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

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

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

$\mathcal{T}$:

\[ s \quad \emptyset \]

\[
\{ c \} \quad \nmid a_{\text{fair}}
\]

\[
\{ b \} \quad \nmid a_{\text{fair}}
\]

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

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

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

$\mathcal{T}$:

\[
\{c\} \not\models a_{\text{fair}} \\
\{b\} \not\models a_{\text{fair}}
\]

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

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

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

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

$CTLFAIR4.4-17$
Example: treatment of $\exists U$

$\mathcal{T}$:

- $s \not\models_{\text{fair}} \exists (\neg b U c)$
- $s \not\models \exists (\neg b U (c \land a_{\text{fair}}))$
- $\text{Sat}(c \land a_{\text{fair}}) = \emptyset$

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

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

$\mathcal{T}$:

$\varnothing \xrightarrow{s} \{c\} \not\models a_{fair}$

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

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

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

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

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

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

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

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?

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

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:

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

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

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:

\[ s \models \exists O \exists (c \lor (b \land a_{\text{fair}})) \]

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

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

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

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:

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

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

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

correct.

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

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.

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

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

\[
\begin{align*}
\text{fair} &= \square \diamond \text{gray} \\
\text{Sat}_{\text{fair}} (\exists (c \cup b)) &= \emptyset
\end{align*}
\]
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.**

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

**Wrong.**

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

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

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

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

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

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

correct.

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

wrong.

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

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

\[
s \not\models _{\text{fair}} \exists \bigcirc \exists (c \cup b)
\]

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

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

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

wrong.

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

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

Wrong.

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

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

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

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

Wrong.

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

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

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

wrong.

\[ \text{fa}ir = \Box \Diamond b \]

\[ s_0 \models \text{fa}ir \]

\[ s_1 \models \text{fa}ir \]

regard state \( s = s_0 \):

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

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

Wrong.

\[
\begin{align*}
\text{fair} &= \Box \Diamond b \\
\text{s}_0 &\models a_{\text{fair}} \\
\text{s}_1 &\models a_{\text{fair}}
\end{align*}
\]

regard state \( s = s_0 \):

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

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

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

wrong.

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

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

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

regard state \( s = s_0 \):

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

↑

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

\( \textit{fair} = \square \diamond b \to \square \diamond c, \quad \text{CTL state formula} \; \Psi \)

\( T : \)

\[ \emptyset \quad \emptyset \]

\[ \{ c \} \quad \{ c \} \quad \{ c \} \]

\[ \{ b \} \]

\[ \square \]

\[ \bigtriangledown \]

\( T \models_{\text{fair}} \exists \square \Psi ? \)
\( fair = \Box \Diamond b \rightarrow \Box \Diamond c \), \( T \models fair \exists \Box \Psi \) ?

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

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

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

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

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

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

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

\textit{fair} = □♦b \rightarrow □♦c, \quad \text{CTL state formula } \Psi

\mathcal{T}:

\begin{align*}
\{c, a\} & \rightarrow \{a\} \\
\{c, a\} & \rightarrow \emptyset \\
\{b, a\} & \rightarrow \emptyset
\end{align*}

digraph \ G_a

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

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

CTL state formula \(\Psi\)

\[\mathcal{T}:\]

\[\{c, a\} \xrightarrow{} \{a\} \xrightarrow{} \varnothing\]

\[\{c, a\} \xrightarrow{} \{a\} \xrightarrow{} \varnothing\]

\[\{b, a\} \xrightarrow{} \varnothing\]

digraph \(G_a\)

doesn’t contain any fair path

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

2. replace \(\Psi\) with a fresh atomic proposition \(a = a_\Psi\)

3. calculate \(Sat_{\text{fair}}(\exists\Box a)\)
∃□Ψ under strong fairness

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

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

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

if all states are labeled by $a$:
	this technique yields a method
to compute $Sat_{fair}(\exists \Box true)$
Treatment of $\exists \Box a$ for FairCTL

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

if all states are labeled by $a$:
this technique yields a method
to compute $Sat_{fair}(\exists \Box true)$

here: explanations only for strong fairness

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

$$fair = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$$
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 $s_0 s_1 \ldots s_n \ldots s_{n+r}$
Treatment of $\exists \Box$ under strong fairness

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

$s \models_{fair} \exists \Box a$ iff there exists a path fragment $s_0 s_1 \ldots s_n \ldots s_{n+r}$ such that $r \geq 1$, $s = s_0$, $s_n = s_{n+r}$ and ...
Treatment of $\exists \Box \cdot \Box$ 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 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 $\exists □$ under strong fairness

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

$s \models_{fair} \exists □ a$ 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.,
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 $0 \leq j \leq n + r$
- 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 $\{s_{n+1}, \ldots, s_{n+r}\} \cap \text{Sat}(c_i) \neq \emptyset$
∃a under strong fairness

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

\begin{itemize}
  \item Π $\models a$
  \item ○ $\not\models a$
\end{itemize}
∃\( a \) under strong fairness

does \( \mathcal{T} \models^\text{fair} \exists \Box a \) hold?

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

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

digraph $G_a$

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

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

digraph $G_a$

$\models \{ b_1 \}$  $\models \{ c_1 \}$

$\models \{ b_2 \}$  $\models \{ c_2 \}$

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

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

digraph $G_a$

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

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

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

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

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

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

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

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

digraph $G_a$

$\exists □ a$ under strong fairness

does $\mathcal{T} \models_{fair} \exists □ a$ hold?
Treatment of $\exists \Box$ under strong fairness

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

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

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

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

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

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

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

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

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

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

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

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

$G_a$: digraph that arises from $\mathcal{T}$ by removing all states $s'$ with $s' \not\models a$
Treatment of $∃□$ under strong fairness

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

$s \models_{\text{fair}} ∃□a$ 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 $:\mathcal{T}$ by removing all states $s'$ with $s' \not\models a$
Treatment of $\exists$ under strong fairness

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

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

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

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

\[
T \xrightarrow{\{c_2\}} \quad \text{digraph } G_a \xrightarrow{\{b_2\}}
\]

\[
\text{fair} = (\Box \Diamond b_1 \rightarrow \Box \Diamond c_1) \land (\Box \Diamond b_2 \rightarrow \Box \Diamond c_2)
\]
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 $\text{Sat}_{\text{fair}}(\exists \Box a)$

$\mathcal{T}$

- $\{c_2\} \rightarrow \{b_2\}$
- $\{b_1\} \rightarrow \{c_1\}$

$\text{digraph } G_a$

- $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$

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

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

$T$

\{ $b_1$ \}

\{ $c_1$ \}

\{ $c_2$ \}

digraph $G_a$

$s_0$

$s_1$

$s_2$

$s_3$

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

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

as $s_0 \ s_1 \ s_2 \ s_1 \ s_2 \ldots \models_{LTL} fair$

$Sat_{fair}(\exists \square a) = \{ s_0, s_1, s_2, s_3 \}$
CTL model checking with fairness

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

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

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

*here:* explanations only for strong fairness

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

weak fairness and combinations of weak/strong fairness can be treated in an analogous way
CTL model checking with fairness

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

*here*: explanations only for strong fairness

<table>
<thead>
<tr>
<th>case 1: unconditional fairness</th>
</tr>
</thead>
</table>

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

- **case 3**: arbitrary strong fairness assumption
  \[
  \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)
  \]

weak fairness and combinations of weak/strong fairness can be treated in an analogous way
∃\(a\) under unconditional fairness

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

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

\[ s \models_{\text{fair}} \exists a \text{ iff } ? \]
∃a under unconditional fairness

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

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

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

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

digraph \ G_a

fairness assumption:

\[ \text{fair} = \Box \diamond c_1 \land \Box \diamond c_2 \]
∃ a under unconditional fairness

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

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

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

digraph \( G_a \)

fairness assumption:
\[ \text{fair} = \Box ♦ c_1 \land \Box ♦ c_2 \]
\[ s \not\models_{\text{fair}} \exists \Box a \]
∃a under unconditional fairness

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

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

digraph \( G_a \)

fairness assumption:
\[ fair = \Box \Diamond c_1 \land \Box \Diamond c_2 \]
\[ s \not\models_{fair} \exists \Box a \]
∃a under unconditional fairness

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

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

digraph \( G_a \)

fairness assumption:

\[ \textit{fair} = \Box \Diamond c_1 \land \Box \Diamond c_2 \]
∃◊a under unconditional fairness

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

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

digraph \( G_a \)

fairness assumption:
\[ \text{fair} = \square \Diamond c_1 \land \square \Diamond c_2 \]
\[ s \models_{\text{fair}} \exists\square a \]
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: $fair = \Box \Diamond b \rightarrow \Box \Diamond c$</td>
<td></td>
</tr>
<tr>
<td>case 3: arbitrary strong fairness assumption</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

**Case 3:**

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

\[ \text{fair} = \square \diamond b \leadsto \square \diamond c \]
Strong fairness: 1 fairness requirement

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

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

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

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 \( G_a \)

\[ s \preceq \emptyset \]
\[ \{c\} \preceq \{b\} \]

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 \( G_a \)
Strong fairness: 1 fairness requirement

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

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

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

digraph \( G_a \)

\[
\{ c \} \quad \{ b \} \quad D
\]

strongly connected node-set \( D \) of \( G_a \) 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 \( G_a |_C \setminus \text{Sat}(b) \)

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

*here:* explanations only for *strong fairness*

<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>unconditional fairness</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>$\textit{fair} = \Box \Diamond b \rightarrow \Box \Diamond c$</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>arbitrary strong fairness assumption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$\textit{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i)$</td>
<td></td>
</tr>
</tbody>
</table>
treatment of $\exists \Box$ for CTL with fairness

does not have an intuitive meaning for

\[ \text{here: explanations only for strong fairness} \]

case 1: unconditional fairness $\checkmark$

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

case 3: arbitrary strong fairness assumption

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

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

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

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

digraph \( G_a \)

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

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

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

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 \( G_a \)

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

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

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

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

digraph \( G_a \)

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

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

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

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

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

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

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

digraph $G_a$

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

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

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

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

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

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

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

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

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

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

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

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

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: $\mathcal{O}(\text{size}(T) \cdot |\text{fair}|)$
Recursive algorithm \textit{CheckFair}(\ldots)
Recursive algorithm *CheckFair(...)*

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

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

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

“false” otherwise
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))

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

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

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

\textbf{choose} j \in \{1, \ldots, k\} \ \text{with} \ C \cap \text{Sat}(c_j) = \emptyset;
Recursive algorithm **CheckFair( . . . )**

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

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

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

pseudo code for **CheckFair**\((C, k, \bigwedge_{1 \leq i \leq k} (□♦ b_i → □♦ c_i))\)

IF \(∀i \in \{1, ..., k\}. \ C \cap Sat(c_i) \neq \emptyset\) THEN return “true” FI
choose \(j \in \{1, ..., k\}\) with \(C \cap Sat(c_j) = \emptyset\);
remove all states in \(Sat(b_j)\);
IF the resulting graph \(G\) is acyclic THEN return “false” FI
FOR ALL nontrivial SCCs \(D\) of \(G\) DO
  IF **CheckFair**\((D, k−1, \bigwedge_{i \neq j} (□♦ b_i → □♦ c_i))\)
  THEN return “true” FI
OD
Recursive algorithm \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{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
    IF $\texttt{CheckFair}(D, k-1, \bigwedge_{i \neq j} (\Box \Diamond b_i \rightarrow \Box \Diamond c_i))$
    THEN return “true” FI
OD
return “false”
\end{verbatim}
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 $\forall i \in \{1, ..., k\}$. $C \cap \text{Sat}(c_i) \neq \emptyset$ 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”
Complexity of \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, \ldots, k\}. \ C \cap Sat(c_i) \neq \emptyset \ \text{THEN return "true" } \text{FI} \\
\text{choose } j \in \{1, \ldots, k\} \text{ with } C \cap Sat(c_j) = \emptyset; \\
\text{remove all states in } 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} \\
\quad \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{OD} \\
\text{return "false"}
\end{align*}

\textit{recurrence} for the time complexity: 

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

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

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 $\text{CheckFair}(D, k-1, \bigwedge_{i \neq j} (\Box◊b_i \rightarrow \Box◊c_i))$ THEN return “true” OD
OD
return “false”

time complexity: $O(\text{size}(C) \cdot k)$
**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.
input: finite transition system $T$
CTL fairness assumption $fair$
CTL formula $\Phi$

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

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

input: finite transition system $T$
CTL fairness assumption $fair$
CTL formula $\Phi$

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

here: preprocessing
transform $\Phi$ into an equivalent CTL formula
in existential normal form
i.e., with the basic modalities $\exists \Diamond$, $\exists U$ and $\exists \Box$
Model checking algorithm for FairCTL

calculate $\text{Sat}_{\text{fair}}(\exists \square \text{true})$;

label all states in $\text{Sat}_{\text{fair}}(\exists \square \text{true})$ with $a_{\text{fair}}$
Model checking algorithm for FairCTL

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

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

\[
Sat_{fair}(\psi) := \ldots
\]

OD
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:

$\exists \Diamond a$ : $Sat_{\text{fair}}(\psi) := Sat(\exists \Diamond (a \land a_{\text{fair}}))$;

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

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

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

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

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

CASE $\psi$ is:

\[ \exists\bigcirc a : Sat_{fair}(\psi) := Sat(\exists\bigcirc(a \land a_{fair})) ; \]
\[ \exists(a_1 U a_2) : Sat_{fair}(\psi) := Sat(\exists(a_1 U(a_2 \land a_{fair})) ; \]
\[ \exists\Box a : Sat_{fair}(\psi) := ... \]

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

OD
Model checking algorithm for FairCTL

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

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

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

CASE $\psi$ is:

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

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

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

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

OD

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

ELSE return “no”

FI
Example: CTL model checking with fairness

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

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

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

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

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

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

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

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

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

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

\[ \Phi = \exists ♦ \forall O (lost \lor del) \]

\[ \equiv \exists ♦ \neg \exists O (\neg lost \land \neg del) \]

existential normal form

\[
\begin{align*}
\text{fair} &= \square ♦ \exists ♦ \text{del} \leadsto \square ♦ \text{c} \quad \text{where } Sat(c) = S \setminus \{\text{error}\} \\
Sat_{\text{fair}}(\exists \square \text{true}) &= Sat(a_{\text{fair}}) = S \setminus \{\text{error}\}
\end{align*}
\]
Example: CTL model checking with fairness

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

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

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

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

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

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

\[ \sim \exists \Diamond \neg \exists \Box \mathbf{a} \]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\[ \iff \exists \diamond \neg \exists \lozenge \ a \]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\leadsto \exists \Diamond \neg \exists \bigcirc a$$

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

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

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

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

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

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

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

\[ \leadsto \exists \Diamond b \]

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

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

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

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

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

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

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

\[ \leadsto \exists \diamond b \]

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

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

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

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

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

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

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

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

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

\[ \leadsto \exists \Box b \]

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

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

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

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

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

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

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

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

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

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

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

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

\[
\leadsto \exists \diamond \; b
\]

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

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

\[
\text{Sat}_{\text{fair}}(\exists \; b) = \text{Sat}(\exists \; (b \land a_{\text{fair}}))
\]

\[
= \{\text{start, try, lost, del}\}
\]
Example: CTL model checking with fairness

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

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

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

\[ \text{Sat}_{\text{fair}}(\exists \Diamond b) = \text{Sat}(\exists \Diamond (b \land a_{\text{fair}})) \]
\[ = \{\text{start, try, lost, del}\} \]
Correct or wrong?

\[ s \Vdash_{\text{fair}} \forall \bigcirc a \iff s \Vdash \forall \bigcirc (a \land a_{\text{fair}}) \]
Correct or wrong?

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

wrong.

\[ \text{fair} = 
\]

\[ \emptyset \]

\[ \{a, b\} \]
Correct or wrong?

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

wrong.

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

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

wrong.

\( \text{fair} = \Box \Diamond b \)

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

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

wrong.

\[ \text{fair} = \Box \Diamond b \]
\[ s \not\models \forall \Box (a \land \text{afair}) \]
\[ s \models_{fair} \forall \Box a \]
Correct or wrong?

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

Wrong.

\[ fair = \Box \Diamond b \]
\[ s \not\models \forall O (a \land a_{fair}) \]
\[ s \models_{fair} \forall O a \]

But correct is:

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

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

Wrong.

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

But correct is:

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

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

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

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

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

correct
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

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

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

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

\text{correct}

\[ s \models_{\text{fair}} \forall a \text{  iff  } s \models_{\text{fair}} \neg \exists \diamond \neg a \]
Correct or wrong?

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

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

correct

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

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

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

correct

\[
\begin{align*}
s \models_{\text{fair}} \forall □ a & \iff s \models_{\text{fair}} \neg △ \neg a \\
& \iff s \not\models_{\text{fair}} △ \neg a \\
& \iff s \not\models △ (\neg a \land a_{\text{fair}})
\end{align*}
\]
Correct or wrong?

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

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

correct

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

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

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

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

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

iff \( s \models \neg \exists \Diamond (\neg a \land a_{\text{fair}}) \equiv \forall \Box (a_{\text{fair}} \rightarrow a) \)
We just saw:

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

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

We just saw:

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

Is the following statement correct?

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

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

Is the following statement correct?

\[
\begin{align*}
    s \models_{\text{fair}} \forall (b \bigcup a) & \iff s \models \forall (b \bigcup (a_{\text{fair}} \rightarrow a))
\end{align*}
\]

Wrong.
Correct or wrong?

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

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

Wrong.

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

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

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

Wrong.

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

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

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

wrong.

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

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

regard \( s \rightarrow s \)
Correct or wrong?

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

\[ \text{false.} \]

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

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

regard \( s \rightarrow s \)

\[ s \not\models_{\text{fair}} \exists \Box \exists \Diamond a \]
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.

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

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

regard \( s \rightarrow s \)

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

(note \( \text{Sat}_{\text{fair}}(\exists \Diamond a) = \emptyset \))
Correct or wrong?

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

Wrong.

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

Remind: \(W = \text{weak until}\)
Correct or wrong?

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

wrong.

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

remind: \( W = \) weak until

wrong.
Correct or wrong?

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

wrong.

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

remind: \( \mathcal{W} = \text{weak until} \)

wrong.

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

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

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.

\[ \text{fair} = \square \lozenge b \]

\[ s \models \exists (a \mathcal{W} (c \land a_{\text{fair}})) \]
Correct or wrong?

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

wrong.

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

remind: \( W = \text{weak until} \)

wrong.

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

\[ s \models \exists (a W (c \land a_{\text{fair}})) \]

\[ s \not\models_{\text{fair}} \exists (a W c) \]
Summary: fairness in CTL
CTL fairness assumptions: formulas similar to LTL

e.g., \( \text{fair} = \land_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i) \)
**Summary: fairness in CTL**

**CTL** fairness assumptions: formulas similar to **LTL**

\[ \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i) \]

**CTL** satisfaction relation with fairness:

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

\[ \pi \models \text{fair} \quad \text{and} \quad \pi \models_{\text{fair}} \varphi \]
**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:

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

Model checking for **CTL** with fairness:
**Summary: fairness in CTL**

**CTL** fairness assumptions: formulas similar to **LTL**

e.g.,\[ \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i) \]

**CTL** satisfaction relation with fairness:

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

Model checking for **CTL** with fairness:

- \( \exists \bigcirc, \exists \bigcup, \forall \bigcirc, \forall \Box \) via **CTL** model checker
Summary: fairness in CTL

**CTL fairness assumptions:** formulas similar to LTL

e.g., \( \text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \phi_i) \)

**CTL satisfaction relation with fairness:**

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

\( \pi \models_{\text{fair}} \text{fair} \) and \( \pi \models_{\text{fair}} \varphi \)

**Model checking for CTL with fairness:**

- \( \exists \Box, \exists U, \forall \Box, \forall \Box \) via CTL model checker
- Analysis of SCCs for \( \exists \Box, \forall U \)
CTL fairness assumptions: formulas similar to LTL

e.g., $\text{fair} = \bigwedge_{1 \leq i \leq k} (\Box \Diamond \psi_i \rightarrow \Box \Diamond \Phi_i)$

CTL satisfaction relation with fairness:

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

model checking for CTL with fairness:

- $\exists \bigcirc$, $\exists U$, $\forall \bigcirc$, $\forall \Box$ via CTL model checker
- analysis of SCCs for $\exists \Box$, $\forall U$
- complexity: $O(\text{size}(T) \cdot |\Phi| \cdot |\text{fair}|)$