Temporal logic CTL⁻: syntax

\[
\Phi ::= \text{tt} \mid \text{ff} \mid \Phi_1 \land \Phi_2 \mid \Phi_1 \lor \Phi_2 \mid [K]\Phi \mid \langle K \rangle \Phi \\
AG \Phi \mid EF \Phi \mid AF \Phi \mid EG \Phi
\]

A formula can be
Temporal logic CTL$^-$: syntax

\[ \Phi ::= \text{tt} | \text{ff} | \Phi_1 \land \Phi_2 | \Phi_1 \lor \Phi_2 | [K]\Phi | \langle K \rangle \Phi \\
AG \Phi | EF \Phi | AF \Phi | EG \Phi \]

A formula can be

- a formula of Hennessy-Milner logic,
Temporal logic $\text{CTL}^-$: syntax

$$\Phi ::= \text{tt} | \text{ff} | \Phi_1 \land \Phi_2 | \Phi_1 \lor \Phi_2 | [K]\Phi | \langle K \rangle \Phi$$
$$AG \Phi | EF \Phi | AF \Phi | EG \Phi$$

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $AG \Phi$, read as “always $\Phi$” or “globally $\Phi$,”
Temporal logic CTL⁻: syntax

\[ \Phi ::= tt \mid ff \mid \Phi_1 \land \Phi_2 \mid \Phi_1 \lor \Phi_2 \mid [K] \Phi \mid \langle K \rangle \Phi \]
\[ \quad \text{AG } \Phi \mid \text{EF } \Phi \mid \text{AF } \Phi \mid \text{EG } \Phi \]

A formula can be

- a formula of Hennessy-Milner logic,
- a formula AG \Phi, read as “always \Phi” or “globally \Phi,”
- a formula EF \Phi, read as “possibly \Phi,”
Temporal logic $\text{CTL}^{-}$: syntax

$$\Phi ::= \text{tt} | \text{ff} | \Phi_1 \land \Phi_2 | \Phi_1 \lor \Phi_2 | [K]\Phi | \langle K \rangle \Phi$$
$$\quad \text{AG } \Phi | \text{EF } \Phi | \text{AF } \Phi | \text{EG } \Phi$$

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $\text{AG } \Phi$, read as “always $\Phi$” or “globally $\Phi$,”
- a formula $\text{EF } \Phi$, read as “possibly $\Phi$,”
- a formula $\text{AF } \Phi$, read as “eventually $\Phi$,”
Temporal logic CTL$^-$: syntax

\[
\Phi ::= \text{tt} | \text{ff} | \Phi_1 \land \Phi_2 | \Phi_1 \lor \Phi_2 | [K]\Phi | \langle K \rangle \Phi \\
AG \Phi | EF \Phi | AF \Phi | EG \Phi
\]

A formula can be

- a formula of Hennessy-Milner logic,
- a formula $AG \Phi$, read as “always $\Phi$” or “globally $\Phi$,”
- a formula $EF \Phi$, read as “possibly $\Phi$,”
- a formula $AF \Phi$, read as “eventually $\Phi$,”
- a formula $EG \Phi$, read as “EG $\Phi$.”
Temporal logic CTL⁻: semantics

A run (of a process $E_0$) is a sequence of transitions of the form

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} E_2 \xrightarrow{a_3} \ldots$$

which is “maximal” in the sense that if it is finite then the final process is unable to do any action.
Temporal logic $\text{CTL}^-$: semantics

A run (of a process $E_0$) is a sequence of transitions of the form

$$E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} E_2 \xrightarrow{a_3} \ldots$$

which is “maximal” in the sense that if it is finite then the final process is unable to do any action.

- $E_0 \models \text{AG } \Phi$  iff  for all runs $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots$, for all $i \geq 0$, $E_i \models \Phi$
- $E_0 \models \text{EF } \Phi$  iff  for some run $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots$, for some $i \geq 0$, $E_i \models \Phi$
- $E_0 \models \text{AF } \Phi$  iff  for all runs $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots$, for some $i \geq 0$, $E_i \models \Phi$
- $E_0 \models \text{EG } \Phi$  iff  for some run $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \ldots$, for all $i \geq 0$, $E_i \models \Phi$
Intuitive meaning

- $E_0 \models AG \Phi$ means "all processes reachable from $E_0$ satisfy $\Phi$."
Intuitive meaning

- $E_0 \models AG \Phi$ means “all processes reachable from $E_0$ satisfy $\Phi$.”
- $E_0 \models EF \Phi$ means “some process reachable from $E_0$ satisfies $\Phi$.”
Intuitive meaning

- $E_0 \models AG \Phi$ means “all processes reachable from $E_0$ satisfy $\Phi$.”
- $E_0 \models EF \Phi$ means “some process reachable from $E_0$ satisfies $\Phi$.”
- $E_0 \models AF \Phi$ means “eventually a process will be reached which satisfies $\Phi$.”
Intuitive meaning

- $E_0 \models AG \Phi$ means “all processes reachable from $E_0$ satisfy $\Phi$.”
- $E_0 \models EF \Phi$ means “some process reachable from $E_0$ satisfies $\Phi$.”
- $E_0 \models AF \Phi$ means “eventually a process will be reached which satisfies $\Phi$.”
- $E_0 \models EG \Phi$ means “some run always satisfies $\Phi$.”
Examples

- $E_0 \models AG \langle - \rangle tt$

- All processes reachable from $E_0$ can do some action.
- $E_0$ is deadlock-free.

- Eventually a process is reached which cannot execute any action.
- $E$ is guaranteed to terminate.

- $AG \langle request \rangle AF \langle granted \rangle tt \wedge \langle - granted \rangle ff$

- All requests will eventually be granted
Examples

- $E_0 \models AG \langle \neg \rangle tt$
- All processes reachable from $E_0$ can do some action. $E_0$ is deadlock-free.
Examples

- $E_0 \models AG \langle \neg \rangle tt$

  All processes reachable from $E_0$ can do some action.  

  $E_0$ is deadlock-free.

- $E_0 \models AF \lnot ff$

  All requests will eventually be granted.
Examples

- $E_0 \models \text{AG } (\neg)tt$
- All processes reachable from $E_0$ can do some action. $E_0$ is deadlock-free.
- $E_0 \models \text{AF } [\neg]ff$
- Eventually a process is reached which cannot execute any action. $E$ is guaranteed to terminate.
Examples

- $E_0 \models AG \langle - \rangle tt$
- All processes reachable from $E_0$ can do some action. $E_0$ is deadlock-free.
- $E_0 \models AF \langle - \rangle ff$
- Eventually a process is reached which cannot execute any action. $E$ is guaranteed to terminate.
- $AG \text{[request]} AF (\langle \text{granted} \rangle tt \land \langle - \text{granted} \rangle ff)$
Examples

- $E_0 \models AG \langle - \rangle tt$
- All processes reachable from $E_0$ can do some action. $E_0$ is deadlock-free.
- $E_0 \models AF \langle - \rangle ff$
- Eventually a process is reached which cannot execute any action. $E$ is guaranteed to terminate.
- $AG \langle request \rangle AF (\langle granted \rangle tt \land \langle - granted \rangle ff)$
- All requests will eventually be granted
Exercise

\[ P \overset{\text{def}}{=} a.P + b.Q \quad Q \overset{\text{def}}{=} c.Q \]

Does \( P \models \Phi \) hold when \( \Phi \) is

<table>
<thead>
<tr>
<th>( Y/N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>EF ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>AG ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>AF ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>EG ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>AG EF ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>AF EG ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>EF AG ( \langle c \rangle tt )</td>
</tr>
<tr>
<td>EG AF ( \langle c \rangle tt )</td>
</tr>
</tbody>
</table>
Exercise

\[ P \overset{\text{def}}{=} a \cdot P + b \cdot Q \quad Q \overset{\text{def}}{=} c \cdot Q \]

Does \( P \models \Phi \) hold when \( \Phi \) is

<table>
<thead>
<tr>
<th>( \langle c \rangle \text{tt} )</th>
<th>Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{EF} \langle c \rangle \text{tt} )</td>
<td>Y</td>
</tr>
<tr>
<td>( \text{AG} \langle c \rangle \text{tt} )</td>
<td>N</td>
</tr>
<tr>
<td>( \text{AF} \langle c \rangle \text{tt} )</td>
<td>N</td>
</tr>
<tr>
<td>( \text{EG} \langle c \rangle \text{tt} )</td>
<td>N</td>
</tr>
<tr>
<td>( \text{AG EF} \langle c \rangle \text{tt} )</td>
<td>Y</td>
</tr>
<tr>
<td>( \text{AF EG} \langle c \rangle \text{tt} )</td>
<td>N</td>
</tr>
<tr>
<td>( \text{EF AG} \langle c \rangle \text{tt} )</td>
<td>Y</td>
</tr>
<tr>
<td>( \text{EG AF} \langle c \rangle \text{tt} )</td>
<td>N</td>
</tr>
</tbody>
</table>
Example: Peterson’s solution to mutual exclusion

\[ B_{1f} = b_{1rf}B_{1f} + b_{1wf}B_{1f} + b_{1wt}B_{1t} \]
\[ B_{1t} = b_{1rt}B_{1t} + b_{1wt}B_{1t} + b_{1wf}B_{1f} \]
\[ B_{2f} = b_{2rf}B_{2f} + b_{2wf}B_{2f} + b_{2wt}B_{2t} \]
\[ B_{2t} = b_{2rt}B_{2t} + b_{2wt}B_{2t} + b_{2wf}B_{2f} \]
\[ K_1 = k_{r1}K_1 + k_{w1}K_1 + k_{w2}K_2 \]
\[ K_2 = k_{r2}K_2 + k_{w2}K_2 + k_{w1}K_1 \]
\[ P_1 = b_{1wt}.req_1.k_{w1}.P_{11} \]
\[ P_{11} = b_{2rt}.P_{11} + b_{2rf}.P_{12} + k_{r2}.P_{11} + k_{r1}.P_{12} \]
\[ P_{12} = \text{enter1.exit1}.b_{1wf}.P_1 \]
\[ P_2 = b_{2wt}.req_2.k_{w1}.P_{21} \]
\[ P_{21} = b_{1rf}.P_{22} + b_{1rt}.P_{21} + k_{r1}.P_{21} + k_{r2}.P_{22} \]
\[ P_{22} = \text{enter2.exit2}.b_{2wf}.P_2 \]
\[ \text{Peterson} = (P_1 \mid P_2 \mid K_1 \mid B_{1f} \mid B_{2f}) \setminus L \]
Specification: temporal properties

- Mutual exclusion
Specification: temporal properties

- Mutual exclusion
- Absence of deadlock
Specification: temporal properties

- Mutual exclusion
- Absence of deadlock
- Absence of starvation
Specification: temporal properties

- Mutual exclusion \( \ AG ([\text{exit1}]\text{ff} \lor [\text{exit2}]\text{ff}) \)
- Absence of deadlock
- Absence of starvation
Specification: temporal properties

- Mutual exclusion \( \text{AG} ([\text{exit1}]\text{ff} \lor [\text{exit2}]\text{ff}) \)
- Absence of deadlock \( \text{AG} \langle - \rangle \text{tt} \)
- Absence of starvation
Specification: temporal properties

- Mutual exclusion \( \text{AG} ([\text{exit}1]\text{ff} \lor [\text{exit}2]\text{ff}) \)
- Absence of deadlock \( \text{AG} \langle - \rangle \text{tt} \)
- Absence of starvation (for P1) \( \text{AG} ([\text{req}1]\text{AF} \langle \text{exit}1 \rangle \text{tt}) \)
Negation is also redundant in CTL$^-$: For every formula $\Phi$ of CTL$^-$ there is a formula $\Phi^c$ such that for every process $E$

$$E \models \Phi^c \text{ iff } E \not\models \Phi$$
Negation is also redundant in CTL\(^-\): For every formula \(\Phi\) of CTL\(^-\) there is a formula \(\Phi^c\) such that for every process \(E\)

\[
E \models \Phi^c \text{ iff } E \nmodels \Phi
\]

\(\Phi^c\) is inductively defined as for HML, plus:

\[
\begin{align*}
(AG \Phi)^c &= EF \Phi^c \\
(EF \Phi)^c &= AG \Phi^c \\
(AF \Phi)^c &= EG \Phi^c \\
(EG \Phi)^c &= AF \Phi^c
\end{align*}
\]
Proposition  For every $E_0$ and for every $\Phi$ of $\text{CTL}^-$:

$$E_0 \models \Phi^c \iff E_0 \not\models \Phi.$$
Proposition  For every $E_0$ and for every $\Phi$ of $\text{CTL}^-$:

$$E_0 \models \Phi^c \text{ iff } E_0 \not\models \Phi.$$ 

Proof: By induction on the structure of $\Phi$. 

...
Proposition  For every $E_0$ and for every $\Phi$ of $\text{CTL}^-$:

$$E_0 \models \Phi^c \text{ iff } E_0 \not\models \Phi.$$ 

Proof: By induction on the structure of $\Phi$.
Case $\Phi = \text{AG} \Phi_1$.

$$E_0 \models (\text{AG} \Phi_1)^c$$
iff $$E_0 \models \text{EF} \Phi_1^c$$
iff for some run $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots$,
for some $i \geq 0$ s.t. $E_i \models \Phi_1^c$
iff for some run $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots$,
for some $i \geq 0$ s.t. $E_i \not\models \Phi_1$
iff not for all run $E_0 \xrightarrow{a_1} E_1 \xrightarrow{a_2} \cdots$,
for all $i \geq 0$ s.t. $E_i \models \Phi_1$
iff $E_0 \not\models \text{AG} \Phi_1$
Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.
- A formula is unsatisfiable if no process satisfies it.
- A formula is valid if all processes satisfy it.
- Two formulas are equivalent if they are satisfied by exactly the same processes.
A formula is satisfiable (realisable) if some process satisfies it.
A formula is unsatisfiable if no process satisfies it.
Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.
- A formula is unsatisfiable if no process satisfies it.
- A formula is valid all processes satisfy it.
Satisfiability, validity, equivalence

- A formula is satisfiable (realisable) if some process satisfies it.
- A formula is unsatisfiable if no process satisfies it.
- A formula is valid if all processes satisfy it.
- Two formulas are equivalent if they are satisfied by exactly the same processes.
Which of the following are valid?

<table>
<thead>
<tr>
<th>Expression</th>
<th>Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG φ → AF φ</td>
<td></td>
</tr>
<tr>
<td>AF φ → AG φ</td>
<td></td>
</tr>
<tr>
<td>AG φ → EG φ</td>
<td></td>
</tr>
<tr>
<td>EG φ → AG φ</td>
<td></td>
</tr>
<tr>
<td>AF φ → EF φ</td>
<td></td>
</tr>
<tr>
<td>EF φ → AF φ</td>
<td></td>
</tr>
<tr>
<td>EG φ → EF φ</td>
<td></td>
</tr>
<tr>
<td>EF φ → EG φ</td>
<td></td>
</tr>
<tr>
<td>AF φ → EG φ</td>
<td></td>
</tr>
<tr>
<td>EG φ → AF φ</td>
<td></td>
</tr>
</tbody>
</table>
Which of the following are valid?

<table>
<thead>
<tr>
<th></th>
<th>Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG $\Phi \rightarrow AF \Phi$</td>
<td>Y</td>
</tr>
<tr>
<td>AF $\Phi \rightarrow AG \Phi$</td>
<td>N</td>
</tr>
<tr>
<td>AG $\Phi \rightarrow EG \Phi$</td>
<td>Y</td>
</tr>
<tr>
<td>EG $\Phi \rightarrow AG \Phi$</td>
<td>N</td>
</tr>
<tr>
<td>AF $\Phi \rightarrow EF \Phi$</td>
<td>Y</td>
</tr>
<tr>
<td>EF $\Phi \rightarrow AF \Phi$</td>
<td>N</td>
</tr>
<tr>
<td>EG $\Phi \rightarrow EF \Phi$</td>
<td>Y</td>
</tr>
<tr>
<td>EF $\Phi \rightarrow EG \Phi$</td>
<td>N</td>
</tr>
<tr>
<td>AF $\Phi \rightarrow EG \Phi$</td>
<td>N</td>
</tr>
<tr>
<td>EG $\Phi \rightarrow AF \Phi$</td>
<td>Y</td>
</tr>
</tbody>
</table>
Exercise

Which of the following are equivalent when $\Phi$, $\Phi_1$ and $\Phi_2$ are arbitrary formulas of $\text{CTL}^-$?

<table>
<thead>
<tr>
<th></th>
<th>Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{AG } (\Phi_1 \land \Phi_2)$</td>
<td>$\text{AG } \Phi_1 \land \text{AG } \Phi_2$</td>
</tr>
<tr>
<td>$\text{EF } (\Phi_1 \land \Phi_2)$</td>
<td>$\text{EF } \Phi_1 \land \text{EF } \Phi_2$</td>
</tr>
<tr>
<td>$\text{AF } (\Phi_1 \land \Phi_2)$</td>
<td>$\text{AF } \Phi_1 \land \text{AF } \Phi_2$</td>
</tr>
<tr>
<td>$\text{AG AG } \Phi$</td>
<td>$\text{AG } \Phi$</td>
</tr>
<tr>
<td>$\text{AF AF } \Phi$</td>
<td>$\text{AF } \Phi$</td>
</tr>
<tr>
<td>$\text{EF EF } \Phi$</td>
<td>$\text{EF } \Phi$</td>
</tr>
<tr>
<td>$\text{AG EF AG } \Phi$</td>
<td>$\text{AG EF } \Phi$</td>
</tr>
<tr>
<td>$\text{AG EF AG EF } \Phi$</td>
<td>$\text{AG EF } \Phi$</td>
</tr>
</tbody>
</table>
Exercise

Which of the following are equivalent when $\Phi$, $\Phi_1$ and $\Phi_2$ are arbitrary formulas of CTL$^{-}$?

<table>
<thead>
<tr>
<th></th>
<th>Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbf{AG} (\Phi_1 \wedge \Phi_2)$</td>
<td>$\mathbf{AG} \Phi_1 \wedge \mathbf{AG} \Phi_2$</td>
</tr>
<tr>
<td>$\mathbf{EF} (\Phi_1 \wedge \Phi_2)$</td>
<td>$\mathbf{EF} \Phi_1 \wedge \mathbf{EF} \Phi_2$</td>
</tr>
<tr>
<td>$\mathbf{AF} (\Phi_1 \wedge \Phi_2)$</td>
<td>$\mathbf{AF} \Phi_1 \wedge \mathbf{AF} \Phi_2$</td>
</tr>
<tr>
<td>$\mathbf{AG} \mathbf{AG} \Phi$</td>
<td>$\mathbf{AG} \Phi$</td>
</tr>
<tr>
<td>$\mathbf{AF} \mathbf{AF} \Phi$</td>
<td>$\mathbf{AF} \Phi$</td>
</tr>
<tr>
<td>$\mathbf{EF} \mathbf{EF} \Phi$</td>
<td>$\mathbf{EF} \Phi$</td>
</tr>
<tr>
<td>$\mathbf{AG} \mathbf{EF} \mathbf{AG} \Phi$</td>
<td>$\mathbf{AG} \mathbf{EF} \Phi$</td>
</tr>
<tr>
<td>$\mathbf{AG} \mathbf{EF} \mathbf{AG} \mathbf{EF} \Phi$</td>
<td>$\mathbf{AG} \mathbf{EF} \Phi$</td>
</tr>
</tbody>
</table>