Model Checking:
Branching-Time Temporal Logic (CTL and CTL*)

Assaf Kfoury

March 23, 2015  (adjusted March 31, 2015)
syntax of computation tree logic (CTL)

\[ \varphi ::= T \mid \bot \mid p \mid \neg \varphi \mid \varphi \land \varphi \mid \varphi \lor \varphi \mid \varphi \rightarrow \varphi \]

propositional logic

| AX \varphi | EX \varphi |
| AF \varphi | EF \varphi |
| AG \varphi | EG \varphi |
| A[\varphi U \varphi] | E[\varphi U \varphi] |
| A[\varphi W \varphi] | E[\varphi W \varphi] |
| A[\varphi R \varphi] | E[\varphi R \varphi] |

“next” state
some “future” state
all “future” states
“until”
“weak until”
“release”
semantics of CTL – [LCS, Section 3.4.2, pp 211-214]

▶ satisfaction of a WFF of CTL is defined relative to
a transition system \( \mathcal{M} \triangleq (S, \rightarrow, L) \) and a state \( s \in S \)

1. \( \mathcal{M}, s \models \top \)
2. \( \mathcal{M}, s \not\models \bot \)
3. \( \mathcal{M}, s \models p \iff p \in L(s) \)
4. \( \mathcal{M}, s \models \neg \varphi \iff \mathcal{M}, s \not\models \varphi \)
5. \( \mathcal{M}, s \models \varphi \land \psi \iff \mathcal{M}, s \models \varphi \) and \( \mathcal{M}, s \models \psi \)
6. \( \mathcal{M}, s \models \varphi \lor \psi \iff \mathcal{M}, s \models \varphi \) or \( \mathcal{M}, s \models \psi \)
7. \( \mathcal{M}, s \models \varphi \rightarrow \psi \iff \mathcal{M}, s \models \psi \) whenever \( \mathcal{M}, s \models \varphi \)
8. $\mathcal{M}, s \models \text{AX} \varphi$ iff for every $s'$ such that $s \rightarrow s'$ we have $\mathcal{M}, s' \models \varphi$

9. $\mathcal{M}, s \models \text{EX} \varphi$ iff there is $s'$ such that $s \rightarrow s'$ and $\mathcal{M}, s' \models \varphi$

10. $\mathcal{M}, s \models \text{AG} \varphi$ iff for every path $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ with $s = s_1$, and for every $s_i$ along $\pi$, we have $\mathcal{M}, s_i \models \varphi$

11. $\mathcal{M}, s \models \text{EG} \varphi$ iff there is a path $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ with $s = s_1$ such that for every $s_i$ along $\pi$, we have $\mathcal{M}, s_i \models \varphi$

12. $\mathcal{M}, s \models \text{AF} \varphi$ iff for every path $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ with $s = s_1$, there is $s_i$ along $\pi$ such that $\mathcal{M}, s_i \models \varphi$

13. $\mathcal{M}, s \models \text{EF} \varphi$ iff there is a path $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ with $s = s_1$ and there is $s_i$ along $\pi$ such that $\mathcal{M}, s_i \models \varphi$
14. $\mathcal{M}, s \models A[\varphi U \psi]$ iff for every path $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ with $s = s_1$ we have $\pi \models \varphi U \psi$
14. $\mathcal{M}, s \models A[\varphi \mathbf{U} \psi]$ iff for every path $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ with $s = s_1$ we have $\pi \models \varphi \mathbf{U} \psi$

what is disturbing about the preceding definition??
see [LCS, Section 3.4.2, p 212, point 13]
14. \( \mathcal{M}, s \models A[\varphi U \psi] \) iff for every path \( \pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots \) with \( s = s_1 \) we have \( \pi \models \varphi U \psi \)

what is disturbing about the preceding definition??
see [LCS, Section 3.4.2, p 212, point 13]

15. \( \mathcal{M}, s \models E[\varphi U \psi] \) iff there is a path \( \pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots \) with \( s = s_1 \) such that \( \pi \models \varphi U \psi \)
semantics of CTL – [LCS, Section 3.4.2, pp 211-214]

14. \( M, s \models A[\varphi U \psi] \) iff for every path \( \pi \triangleq s_1 \to s_2 \to s_3 \to \cdots \) with \( s = s_1 \) we have \( \pi \models \varphi U \psi \)

what is disturbing about the preceding definition??
see [LCS, Section 3.4.2, p 212, point 13]

15. \( M, s \models E[\varphi U \psi] \) iff there is a path \( \pi \triangleq s_1 \to s_2 \to s_3 \to \cdots \) with \( s = s_1 \) such that \( \pi \models \varphi U \psi \)

again, what is disturbing about the preceding definition??
see [LCS, Section 3.4.2, p 212, point 14]
finally $P$  

globally $P$  

next $P$  

$P$ until $q$  

$A[F_P]$  

$A[G_P]$  

$A[X_P]$  

$A[U_P][q]$  

$E[F_P]$  

$E[G_P]$  

$E[X_P]$  

$E[U_P][q]$
useful intuitive English qualifiers

- “potentially \( \varphi \)” = \( EF \varphi \)
- “inevitably \( \varphi \)” = \( AF \varphi \)
- “potentially always \( \varphi \)” = \( EG \varphi \)
- “invariantly \( \varphi \)” = \( AG \varphi \)
syntax of CTL* – [LCS, Section 3.5, pp 217 and on]

▶ state formulas

\[ \phi ::= \top \mid p \mid \neg \phi \mid (\phi \land \phi) \mid A[\alpha] \mid E[\alpha] \]

▶ path formulas

\[ \alpha ::= \phi \mid \neg \alpha \mid (\alpha \land \alpha) \mid X \alpha \mid F \alpha \mid G \alpha \mid (\alpha U \alpha) \]

▶ LTL is a “subset” of CTL*

because a LTL formula \( \alpha \) is equivalent to the CTL* formula \( A[\alpha] \)

(this requires a rigorous proof, omitted in the book, based on the formal semantics of CTL*, in the following slides)

▶ CTL is a subset of CTL*

because we can restrict paths formulas to be of the form

\[ \alpha ::= X \phi \mid F \phi \mid G \phi \mid (\phi U \phi) \]

(check that this restriction on \( \alpha \) corresponds to enforcing the requirement that every temporal connective must be coupled with a quantifier)
syntax of CTL* – [LCS, Section 3.5, pp 217 and on]

- state formulas

\[
\varphi ::= \top \mid p \mid \neg \varphi \mid (\varphi \land \varphi) \mid A[\alpha] \mid E[\alpha]
\]
syntax of CTL* – [LCS, Section 3.5, pp 217 and on]

- **state formulas**
  \[ \varphi ::= \top \mid p \mid \neg \varphi \mid (\varphi \land \varphi) \mid A[\alpha] \mid E[\alpha] \]

- **path formulas**
  \[ \alpha ::= \varphi \mid \neg \alpha \mid (\alpha \land \alpha) \mid X\alpha \mid F\alpha \mid G\alpha \mid (\alpha U \alpha) \]
syntax of CTL* – [LCS, Section 3.5, pp 217 and on]

▶ state formulas

\[ \varphi ::= \top \mid p \mid \neg \varphi \mid (\varphi \land \varphi) \mid A[\alpha] \mid E[\alpha] \]

▶ path formulas

\[ \alpha ::= \varphi \mid \neg \alpha \mid (\alpha \land \alpha) \mid X \alpha \mid F \alpha \mid G \alpha \mid (\alpha U \alpha) \]

▶ LTL is a “subset” of CTL*

because a LTL formula \( \alpha \) is equivalent to the CTL* formula \( A[\alpha] \)

(this requires a rigorous proof, omitted in the book, based on the formal semantics of CTL*, in the following slides)
syntax of CTL* – [LCS, Section 3.5, pp 217 and on]

▶ state formulas

\[ \varphi ::= \top \mid p \mid \neg \varphi \mid (\varphi \land \varphi) \mid A[\alpha] \mid E[\alpha] \]

▶ path formulas

\[ \alpha ::= \varphi \mid \neg \alpha \mid (\alpha \land \alpha) \mid X\alpha \mid F\alpha \mid G\alpha \mid (\alpha U \alpha) \]

▶ LTL is a “subset” of CTL*

because a LTL formula \( \alpha \) is equivalent to the CTL* formula \( A[\alpha] \)

(this requires a rigorous proof, omitted in the book, based on the formal semantics of CTL*, in the following slides)

▶ CTL is a subset of CTL*

because we can restrict paths formulas to be of the form

\[ \alpha ::= X\varphi \mid F\varphi \mid G\varphi \mid (\varphi U \varphi) \]

(check that this restriction on \( \alpha \) corresponds to enforcing the requirement that every temporal connective must be coupled with a quantifier)
semantics of CTL* – not in [LCS]

- satisfaction of a **state formula** of CTL* is defined relative to
a transition system \( M \triangleq (S, \rightarrow, L) \) and a state \( s \in S \)

1. \( M, s \models \top \)
2. \( M, s \not\models \bot \)
3. \( M, s \models p \) iff \( p \in L(s) \)
4. \( M, s \models \neg \varphi \) iff \( M, s \not\models \varphi \)
5. \( M, s \models \varphi_1 \land \varphi_2 \) iff \( M, s \models \varphi_1 \) and \( M, s \models \varphi_2 \)
6. \( M, s \models A \alpha \) iff \( M, \pi \models \alpha \) for every path \( \pi \) starting at \( s \)
7. \( M, s \models E \alpha \) iff \( M, \pi \models \alpha \) for some path \( \pi \) starting at \( s \)
semantics of CTL* – not in [LCS]

- satisfaction of a **path formula** of CTL* is defined relative to a transition system \( \mathcal{M} \triangleq (S, \rightarrow, L) \) and a path \( \pi \triangleq s_1 \rightarrow s_2 \rightarrow \cdots \)

1. \( \mathcal{M}, \pi \models \varphi \) iff \( \mathcal{M}, s_1 \models \varphi \)

2. \( \mathcal{M}, \pi \models \neg \alpha \) iff \( \mathcal{M}, \pi \not\models \alpha \)

3. \( \mathcal{M}, \pi \models \alpha_1 \land \alpha_2 \) iff \( \mathcal{M}, \pi \models \alpha_1 \) and \( \mathcal{M}, \pi \models \alpha_2 \)

4. \( \mathcal{M}, \pi \models X \alpha \) iff \( \mathcal{M}, \pi^2 \models \alpha \)

5. \( \mathcal{M}, \pi \models F \alpha \) iff there is \( n \geq 1 \) such that \( \mathcal{M}, \pi^n \models \alpha \)

6. \( \mathcal{M}, \pi \models G \alpha \) iff for every \( n \geq 1 \) it holds that \( \mathcal{M}, \pi^n \models \alpha \)

7. \( \mathcal{M}, \pi \models \alpha_1 U \alpha_2 \) iff there is \( n \geq 1 \) such that \( \mathcal{M}, \pi^n \models \alpha_2 \) for every \( 1 \leq k < n \) it holds that \( \mathcal{M}, \pi^k \models \alpha_1 \)
comparing LTL, CTL, and CTL*

- $\varphi_{1,\text{LTL}} \triangleq G \neg p$ and $\varphi_{1,\text{CTL}} \triangleq A G \neg p$ express the same property “$p$ never holds”

- $\varphi_{2,\text{LTL}} \triangleq G (p \rightarrow F q)$ and $\varphi_{2,\text{CTL}} \triangleq A G (p \rightarrow A F q)$ express the same property “whenever $p$ happens, $q$ eventually happens”
comparing LTL, CTL, and CTL* (continued)

▶ useful fact to prove non-equivalences between LTL and CTL.

FACT: Let $M$ and $M'$ be models of LTL (same as models of CTL) such that $\text{Paths}(M') \subseteq \text{Paths}(M)$ – or $\text{Traces}(M') \subseteq \text{Traces}(M)$ – and let $\varphi$ be a WFF of LTL.

If $M \models \varphi$ then $M' \models \varphi$.

The preceding fact does not hold if $\varphi$ is a WFF of CTL.

▶ Exercise: Write a WFF of CTL which is a counter-example showing that the preceding fact fails for CTL.
useful fact to prove non-equivalences between LTL and CTL.

**FACT:** Let $\mathcal{M}$ and $\mathcal{M}'$ be models of LTL (same as models of CTL) such that $\text{Paths}(\mathcal{M}') \subseteq \text{Paths}(\mathcal{M})$ – or $\text{Traces}(\mathcal{M}') \subseteq \text{Traces}(\mathcal{M})$ – and let $\varphi$ be a WFF of LTL.

If $\mathcal{M} \models \varphi$ then $\mathcal{M}' \models \varphi$.

The preceding fact does not hold if $\varphi$ is a WFF of CTL.

**Exercise:** Write a WFF of CTL which is a counter-example showing that the preceding fact fails for CTL.

$\varphi_{3,\text{LTL}} \triangleq F \ X p$ is not equivalent to $\varphi_{3,\text{CTL}} \triangleq A F A X p$

$\varphi_{3,\text{CTL}}$ can distinguish between two transition systems which $\varphi_{3,\text{LTL}}$ cannot.
useful fact to prove non-equivalences between LTL and CTL.

**FACT:** Let $\mathcal{M}$ and $\mathcal{M}'$ be models of LTL (same as models of CTL) such that $\text{Paths}(\mathcal{M}') \subseteq \text{Paths}(\mathcal{M})$ – or $\text{Traces}(\mathcal{M}') \subseteq \text{Traces}(\mathcal{M})$ – and let $\varphi$ be a WFF of LTL.

If $\mathcal{M} \models \varphi$ then $\mathcal{M}' \models \varphi$.

The preceding fact does **not** hold if $\varphi$ is a WFF of CTL.

**Exercise:** Write a WFF of CTL which is a counter-example showing that the preceding fact fails for CTL.

$\varphi_{3,\text{LTL}} \triangleq \text{F X } p$ is **not equivalent** to $\varphi_{3,\text{CTL}} \triangleq \text{A F A X } p$

$\varphi_{3,\text{CTL}}$ can distinguish between two transition systems which $\varphi_{3,\text{LTL}}$ cannot

**stronger fact:** $\varphi_{3,\text{CTL}}$ can distinguish between two transition systems which no LTL formula can

$\varphi_{4,\text{LTL}} \triangleq \text{F G } p$ is **not equivalent** to $\varphi_{4,\text{CTL}} \triangleq \text{A F A G } p$

$\varphi_{4,\text{LTL}}$ holds in a transition system where $\varphi_{4,\text{CTL}}$ does not

**stronger fact:** $\varphi_{4,\text{LTL}}$ expresses a property which no CTL formula can
comparing LTL, CTL, and CTL* (continued)

- $\varphi_{5,\text{LTL}} \triangleq Xp$ is not equivalent to $\varphi_{5,\text{CTL}} \triangleq E Xp$


Question: Why is $\psi \triangleq E Xp \land A F Gp$ not a WFF in the syntax of CTL?
comparing LTL, CTL, and CTL* (continued)

- $\varphi_{5,\text{LTL}} \triangleq Xp$ is not equivalent to $\varphi_{5,\text{CTL}} \triangleq E Xp$

- **No** LTL formula and **no** CTL formula is equivalent to the CTL* formula $\psi \triangleq E XP \land AFGp$

*Question: Why is $\psi$ not a WFF in the syntax of CTL?*