CS 512, Spring 2018, Handout 14

Model-Checking: Temporal Logic CTL*

Assaf Kfoury

February 22, 2018

syntax of CTL*

Following [PMC, Sect 6.8, pp 422-427] rather than [LCS, Sect 3.5, pp 217-220] :

- **state formulas** (ranged by upper case Greek letters, Φ, Ψ, $\ldots$) with $p \in \mathrm{AP}$:

$$\Phi \ ::= \ \mathtt{true} \ \mid \ p \ \mid \ \neg\Phi \ \mid \ \Phi_1 \wedge \Phi_2 \ \mid \ \exists\varphi$$

- **path formulas** (ranged by lower case Greek letters, φ, ψ, $\ldots$):

$$\varphi \ ::= \ \Phi \ \mid \ \neg\varphi \ \mid \ \varphi_1 \wedge \varphi_2 \ \mid \ \bigcirc \varphi \ \mid \ \varphi_1 \ \mathbb{U} \ \varphi_2$$

syntax of CTL*

Following [PMC, Sect 6.8, pp 422-427] rather than [LCS, Sect 3.5, pp 217-220]:

- **state formulas** (ranged by upper case Greek letters, Φ, Ψ, $\ldots$) with $p \in \mathrm{AP}$:

$$\Phi \ ::= \ \mathtt{true} \ \mid \ p \ \mid \ \neg\Phi \ \mid \ \Phi_1 \wedge \Phi_2 \ \mid \ \exists\varphi$$

- **path formulas** (ranged by lower case Greek letters, φ, ψ, $\ldots$):

$$\varphi \ ::= \ \Phi \ \mid \ \neg\varphi \ \mid \ \varphi_1 \wedge \varphi_2 \ \mid \ \bigcirc\,\varphi \ \mid \ \varphi_1 \,\mathbb{U}\, \varphi_2$$

- **shorthands** (useful when using small set of primitive connectives as in [PMC])

  (1) usual propositional connectives: $\rightarrow$, $\vee$, $\leftrightarrow$, $\ldots$, in terms of $\{\neg, \wedge\}$

  (2) $\Diamond\varphi \ \triangleq \ \mathtt{true}\,\mathbb{U}\,\varphi$

  (3) $\Box\varphi \ \triangleq \ \neg\Diamond\neg\varphi$

  (4) $\forall\varphi \ \triangleq \ \neg\exists\neg\varphi$

Similar shorthands as in (1), (2), and (3) hold for LTL and CTL
(see [PMC, comments between Examples 6.2 and 6.3, pp 318-319]),
but shorthand in (4) cannot be used in CTL (why?).

semantics of CTL* (syntax directed)

From [PMC, Definition 6.81, page 423],

the semantics of CTL* are omitted in [LCS, Section 3.5, pages 217-221]:

- satisfaction of a **state formula** of CTL* is defined relative to a transition system TS $\triangleq (S, \mathsf{Act}, \rightarrow, I, \mathsf{AP}, L)$ and a state $s \in S$

1. $\mathsf{TS}, s \models \texttt{true}$
2. $\mathsf{TS}, s \models p$ iff $p \in L(s)$
3. $\mathsf{TS}, s \models \neg\Phi$ iff $\mathsf{TS}, s \not\models \Phi$
4. $\mathsf{TS}, s \models \Phi \wedge \Psi$ iff $\mathsf{TS}, s \models \Phi$ and $\mathsf{TS}, s \models \Psi$
5. $\mathsf{TS}, s \models \exists\,\varphi$ iff $\mathsf{TS}, \pi \models \varphi$ for some path π starting at s

semantics of CTL* (syntax directed)

- satisfaction of a **path formula** of CTL* is defined relative to a transition system $\mathsf{TS} \triangleq (S, \mathsf{Act}, \rightarrow, I, \mathsf{AP}, L)$ and a path $\pi \triangleq s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \cdots$

1. $\mathsf{TS}, \pi \models \Phi$ iff $\mathsf{TS}, s_0 \models \Phi$
2. $\mathsf{TS}, \pi \models \neg\varphi$ iff $\mathsf{TS}, \pi \not\models \varphi$
3. $\mathsf{TS}, \pi \models \varphi_1 \wedge \varphi_2$ iff $\mathsf{TS}, \pi \models \varphi_1$ and $\mathsf{TS}, \pi \models \varphi_2$
4. $\mathsf{TS}, \pi \models \bigcirc\, \varphi$ iff $\mathsf{TS}, \pi[1\ldots] \models \varphi$
5. $\mathsf{TS}, \pi \models \varphi_1 \ \mathbb{U}\ \varphi_2$ iff there is $n \geqslant 0$ such that $\mathsf{TS}, \pi[n\ldots] \models \varphi_2$ and for every $0 \leqslant k < n$ it holds that $\mathsf{TS}, \pi[k\ldots] \models \varphi_1$

semantics of CTL*

- CTL* semantics for transition systems TS $\triangleq (S, \text{Act}, \rightarrow, I, \text{AP}, L)$ from [PMC, Definition 6.82, page 423] :
  - given a **state formula** Φ of CTL*:

    $$\text{TS} \models \Phi \qquad \text{iff} \qquad \text{TS}, s \models \Phi \quad \text{for every } s \in I$$

  - given a **path formula** φ of CTL*:

    $$\text{TS} \models \varphi \qquad \text{iff} \qquad \text{TS}, \pi \models \varphi \quad \text{for every path } \pi \text{ starting at some } s \in I$$

LTL and CTL are sublogics of CTL*

- LTL is a "subset" of CTL*

  because a LTL formula φ is equivalent to the CTL* formula $\forall\varphi$

  (this requires a rigorous proof, [PMC, Theorem 6.83, page 424] , based on the formal semantics of CTL*

LTL and CTL are sublogics of CTL*

- LTL is a "subset" of CTL*

  because a LTL formula φ is equivalent to the CTL* formula $\forall\varphi$

  (this requires a rigorous proof, [PMC, Theorem 6.83, page 424] , based on the formal semantics of CTL*

- CTL is a subset of CTL*

  because we can restrict paths formulas to be of the form

  $$\varphi \;::=\; \bigcirc\,\Phi \quad | \quad | \quad \Phi \,\mathbb{U}\, \Phi$$

  (check that this restriction on φ corresponds to enforcing the requirement that every **temporal connective** must be coupled with a **quantifier**)

(THIS PAGE INTENTIONALLY LEFT BLANK)