CS 512, Spring 2018, Handout 10

Model Checking:
Branching-Time Temporal Logic (CTL)

Assaf Kfoury

February 12, 2018 (adjusted February 15, 2018)

reading assignment

- [PMC, Sections 6.1+6.2, pages 313-334] :
  Start from the very beginning and focus on motivation and examples.
  These are 30 pages that become increasingly more complicated.
- [LCS, Section 3.4, pages 207-216] :

  Considerable overlap with the material in [PMC], with fewer examples.
- Differences in the syntax of LTL and CTL between [PMC] and [LCS]:

modality	where in [PMC]	where in [LCS]
“next”	$\bigcirc$, page 231	X, page 176
“until”	U, page 231	U, page 176
“eventually”	$\Diamond$, page 232	F, page 176
“always”	$\Box$, page 232	G, page 176
“for all”	$\forall$, page 317	A, page 208
“there is”	$\exists$, page 317	E, page 208

- We follow notation and conventions of [PMC] rather than [LCS] – except that we use “$\mathbb{U}$” instead of “U” to avoid any possible confusion with set union “$\cup$”.

syntax of computation tree logic (CTL)

- according to [LCS, Definition 3.12, page 208], where p ranges over AP:

$\varphi \ ::= \ \texttt{true} \mid \texttt{false} \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \to \varphi$	propositional logic
$\mid \ \forall\bigcirc\,\varphi \ \mid \ \exists\bigcirc\,\varphi$	"next" state
$\mid \ \forall\Diamond\,\varphi \ \mid \ \exists\Diamond\,\varphi$	some "future" state
$\mid \ \forall\Box\,\varphi \ \mid \ \exists\Box\,\varphi$	all "future" states
$\mid \ \forall[\varphi \ \mathbb{U} \ \varphi] \ \mid \ \exists[\varphi \ \mathbb{U} \ \varphi]$	"until"
$\mid \ \forall[\varphi\,\mathsf{W}\,\varphi] \ \mid \ \exists[\varphi\,\mathsf{W}\,\varphi]$	"weak until"
$\mid \ \forall[\varphi\,\mathsf{R}\,\varphi] \ \mid \ \exists[\varphi\,\mathsf{R}\,\varphi]$	"release"

semantics of CTL

- following [LCS, Section 3.4.2, pp 211-214] .
- satisfaction of a WFF of CTL is defined relative to a transition system $\mathsf{TS} \triangleq (S, \mathsf{Act}, \rightarrow, I, \mathsf{AP}, L)$ and a state $s \in S$

1. $\mathsf{TS}, s \models \mathtt{true}$
2. $\mathsf{TS}, s \not\models \mathtt{false}$
3. $\mathsf{TS}, s \models p$ iff $p \in L(s)$
4. $\mathsf{TS}, s \models \neg\varphi$ iff $\mathsf{TS}, s \not\models \varphi$
5. $\mathsf{TS}, s \models \varphi \wedge \psi$ iff $\mathsf{TS}, s \models \varphi$ and $\mathsf{TS}, s \models \psi$
6. $\mathsf{TS}, s \models \varphi \vee \psi$ iff $\mathsf{TS}, s \models \varphi$ or $\mathsf{TS}, s \models \psi$
7. $\mathsf{TS}, s \models \varphi \rightarrow \psi$ iff $\mathsf{TS}, s \models \psi$ whenever $\mathsf{TS}, s \models \varphi$

semantics of CTL

8.	TS, $s \models \forall\bigcirc\,\varphi$	iff	for every s' such that $s \to s'$ we have TS, $s' \models \varphi$
9.	TS, $s \models \exists\bigcirc\,\varphi$	iff	there is s' such that $s \to s'$ and TS, $s' \models \varphi$
10.	TS, $s \models \forall\Box\,\varphi$	iff	for every path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$, and for every s_i along π, we have TS, $s_i \models \varphi$
11.	TS, $s \models \exists\Box\,\varphi$	iff	there is a path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ such that for every s_i along π, we have TS, $s_i \models \varphi$
12.	TS, $s \models \forall\Diamond\,\varphi$	iff	for every path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$, there is s_i along π such that TS, $s_i \models \varphi$
13.	TS, $s \models \exists\Diamond\,\varphi$	iff	there is a path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ and there is s_i along π such that TS, $s_i \models \varphi$

semantics of CTL

14. TS, $s \models \forall[\varphi \; \mathbb{U} \; \psi]$ iff for every path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ we have $\pi \models \varphi \; \mathbb{U} \; \psi$

semantics of CTL

14. TS, $s \models \forall[\varphi \ \mathbb{U} \ \psi]$ iff for every path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ we have $\pi \models \varphi \ \mathbb{U} \ \psi$

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

14. $\mathsf{TS}, s \models \forall[\varphi \;\mathbb{U}\; \psi]$ iff for every path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ we have $\pi \models \varphi \;\mathbb{U}\; \psi$

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

15. $\mathsf{TS}, s \models \exists[\varphi \;\mathbb{U}\; \psi]$ iff there is a path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ such that $\pi \models \varphi \;\mathbb{U}\; \psi$

semantics of CTL

14. TS, $s \models \forall[\varphi \ \mathbb{U} \ \psi]$ iff for every path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ we have $\pi \models \varphi \ \mathbb{U} \ \psi$

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

15. TS, $s \models \exists[\varphi \ \mathbb{U} \ \psi]$ iff there is a path $\pi \triangleq s_1 \to s_2 \to s_3 \to \cdots$ with $s = s_1$ such that $\pi \models \varphi \ \mathbb{U} \ \psi$

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

useful intuitive English qualifiers

- "potentially φ" $= \exists\Diamond\varphi$
- "inevitably φ" $= \forall\Diamond\varphi$
- "potentially always φ" $= \exists\Box\varphi$
- "invariantly φ" $= \forall\Box\varphi$

once more: syntax of computation tree logic (CTL)

- now according to [PMC, Definition 6.1, page 317] , a ranges over AP:

$$\Phi \;::=\; \texttt{true} \;\big|\; a \;\big|\; \neg\Phi \;\big|\; \Phi_1 \wedge \Phi_2 \;\big|\; \exists\varphi \;\big|\; \forall\varphi \qquad \text{state formulas}$$

$$\varphi \;::=\; \bigcirc\Phi \;\big|\; \Phi_1 \,\mathbb{U}\, \Phi_2 \qquad \text{path formulas}$$

once more: semantics of CTL

- now according to [PMC, Definition 6.4, page 320].
- satisfaction of state formulas and path formulas is defined relative to a transition system TS $\triangleq (S, \text{Act}, \rightarrow, I, \text{AP}, L)$, state $s \in S$, and path π in TS:

1. $s \models \texttt{true}$
2. $s \models a$ iff $a \in L(s)$
3. $s \models \neg\Phi$ iff $s \not\models \Phi$
4. $s \models \Phi \wedge \Psi$ iff $s \models \Phi$ and $s \models \Psi$
5. $s \models \exists\varphi$ iff $\pi \models \varphi$ for *some* path π starting at s
6. $s \models \forall\varphi$ iff $\pi \models \varphi$ for *every* path π starting at s
7. $\pi \models \bigcirc\Phi$ iff $\pi[1] \models \Phi$
8. $\pi \models \Phi \, \mathsf{U} \, \Psi$ iff $\pi[j] \models \Psi$ for some $j \geqslant 0$ and $\pi[k] \models \Phi$ for every $0 \leqslant k < j$

where for path $\pi \triangleq s_0\ s_1\ s_2\ \cdots$ and integer $i \geqslant 0$, we denote s_i by $\pi[i]$.

(THIS PAGE INTENTIONALLY LEFT BLANK)