FMSoft

Lecture 6, part II — CTL*

(pre-lecture version)

Tadeusz Litak

November 20, 2018

Informatik 8, FAU Erlangen-Nürnberg

- In order to compare LTL and CTL systematically, let us consider something still more powerful
- CTL*(Emerson and Clarke 1986), a language whose syntax incorporates both
  - explicit path formulas and
  - explicit state formulas
- Price: model checking no longer polynomial in $|\psi|$
- In fact, it can be done by reduction to model checking for LTL that Christoph is going to discuss

- Syntax:

$$\begin{array}{rl} \text{state formulas} & \phi, \psi ::= \top \mid \mathsf{p} \mid \neg\phi \mid \phi \wedge \psi \mid \mathsf{E}[\alpha] \mid \mathsf{A}[\alpha] \\ \text{path formulas} & \alpha, \beta ::= \phi \mid \neg\alpha \mid \alpha \wedge \beta \mid \mathsf{X}\alpha \mid \alpha \mathsf{U} \beta \end{array}$$

- usual abbreviations for path and state connectives
- we could also define $\mathsf{A}[\alpha]$ as $\neg\mathsf{E}[\neg\alpha]$
- we could also use different symbols for state and path operators

  I'm worried this would increase rather than decrease confusion though

- $\mathcal{M}, s \models \top$ always
- $\mathcal{M}, s \models \mathsf{p}$ if $\mathsf{p} \in L(s)$
- $\mathcal{M}, s \models \neg\phi$ if $\mathcal{M}, s \not\models \phi$
- $\mathcal{M}, s \models \phi \wedge \psi$ if $\mathcal{M}, s \models \phi$ and $\mathcal{M}, s \models \psi$
- $\mathcal{M}, s \models \mathsf{E}[\alpha]$ if exists $\pi \in \Pi(s)$ s.t. $\mathcal{M}, \pi \models \alpha$
- $\mathcal{M}, s \models \mathsf{A}[\alpha]$ if for all $\pi \in \Pi(s)$ s.t. $\mathcal{M}, \pi \models \alpha$

- $\mathcal{M}, \pi \models \phi$ if $\mathcal{M}, \pi(0) \models \phi$
- $\mathcal{M}, \pi \models \neg\alpha$ if $\mathcal{M}, \pi \not\models \alpha$
- $\mathcal{M}, \pi \models \alpha \wedge \beta$ if $\mathcal{M}, \pi \models \alpha$ and $\mathcal{M}, \pi \models \beta$
- $\mathcal{M}, \pi \models \mathsf{X}\alpha$ if $\mathcal{M}, \pi_1 \models \alpha$
- $\mathcal{M}, \pi \models \alpha \mathsf{U} \beta$ if $\exists n \in \mathbb{N}. \mathcal{M}, \pi_n \models \beta$ and $\forall i < n. \mathcal{M}, \pi_i \models \alpha$

- Standard exercise: work out clauses for other connectives

Other logics so far: fragments

- What are LTL formulas equivalent to?
- ...subset of the form $\mathsf{A}[\alpha']$, where

$$\alpha', \beta' ::= \top \mid \mathsf{p} \mid \neg\alpha' \mid \alpha' \wedge \beta' \mid \mathsf{X}\alpha' \mid \alpha'\mathsf{U}\beta'$$

(only universally quantified path formulas)

- What are CTL formulas equivalent to?
- ...subset of state formulas of the form

$$\phi, \psi ::= \top \mid \mathsf{p} \mid \neg\phi \mid \phi \wedge \psi \mid \mathsf{E}[\alpha] \mid \mathsf{A}[\alpha]$$
$$\alpha ::= \mathsf{X}\phi \mid \mathsf{F}\phi \mid \mathsf{G}\phi \mid \phi\mathsf{U}\psi$$

  - no boolean combinations of path formulas
  - no nesting of path formulas

FCTL and CTL^f in CTL^*

- Regarding $\mathsf{E}_C\mathsf{G}\phi$, C is a legal CTL^* path formula ...
- ...translate the whole thing to $\mathsf{E}[C \wedge \mathsf{G}\phi]$
- Regarding CTL^f, $\mathsf{E}[\phi\mathsf{G}\psi]$ ...
- ...is expressible as $\mathsf{E}[\mathsf{GF}\psi \wedge \mathsf{G}\phi]$

Comparing logics

- Any $\Gamma \in \{\mathsf{LTL}, \mathsf{CTL}, \mathsf{FCTL}, \mathsf{CTL}^f, \mathsf{CTL}^*\}$ can be treated as subset of (state formulas of) CTL^*

  recall we identify $\alpha \in \mathsf{LTL}$ with $\mathsf{A}[\alpha]$

- Write $\Gamma \subseteq \Gamma'$ (Γ' is more expressive than or refines Γ) if

$$\forall \phi \in \Gamma . \exists \psi \in \Gamma' . \phi \equiv \psi$$

- For $\mathsf{CTL} \nsubseteq \mathsf{LTL}$ ...
- ...consider reachability $\mathsf{AGEF}\,\mathtt{deadlock}$. Proof: blackboard

  note you are supposed to be able to reproduce the blackboard proofs

- For $\mathsf{FCTL} \cap \mathsf{CTL}^f \nsubseteq \mathsf{CTL} \cup \mathsf{LTL}$ ...
- ...consider $\mathsf{E}[\mathsf{GF}\,\mathtt{busy}]$. Proof: blackboard for LTL

  But what if we flip satisfying and refuting?

- Recall: $\mathsf{E}_{\mathsf{GF}\mathtt{busy}}\top$ in FCTL and $\mathsf{E}[\top\mathsf{G}\,\mathtt{busy}]$ in CTL^f

- Recall that CTL differed from CTL^* by allowing
  - no boolean combinations of path formulas
  - no nesting of path formulas
- The first restriction is irrelevant for expressivity ...
- ...relevant for succinctness and complexity of model checking
- For more information, cf. yet another fragment of CTL^*...
- ...called CTL^+ by Emerson and Halpern

  E. A. Emerson and J. Y. Halpern. Decision procedures and expressiveness in the temporal logic of branching time. *Journal of Computer and System Sciences*, 30:1–24, 1985

  CTL^+allows boolean combinations of path formulas inside a path quantifier but no nesting of them