CS 512: Formal Methods Instructor: Prof. Assaf Kfoury

Lecture 11

Tuesday, Feb. 27. 2018

Spring 2018 Scribed by Wonyl Choi

1 Class Announcements

- The mid-term exam (take-home) is scheduled in Thursday, March 1st. *No Lecture* on that day. The exam questions will be posted and solutions must be send via E-mail directly.
- Hints for some problems of Assignment 5 are added.

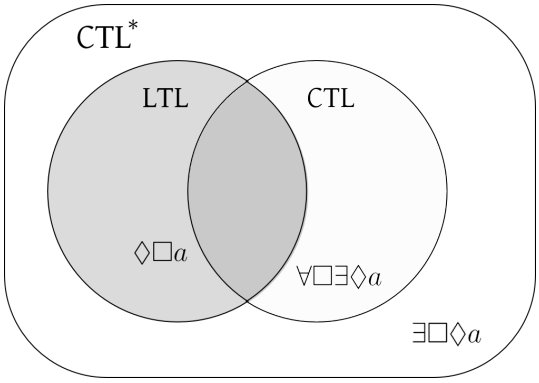
  (*On problem 4 [PMC, page 435] Exercise 6.8*)
  Define transition systems TS_1 and TS_2 and a CTL formula Φ such that

  $$\mathsf{Trace}(\mathsf{TS}_1) = \mathsf{Trace}(\mathsf{TS}_2) \text{ but } \mathsf{TS}_1 \vDash \Phi \text{ and } \mathsf{TS}_2 \nvDash \Phi.$$

- Handout 15 is revised and modified.

2 Recap. Comparison of LTL, CTL, and CTL*

[Handout 15, p.2–p.5.]



- There exists some overlap of LTL and CTL; however, neither logic subsumes the other. For example, there is no CTL formula equivalent to the LTL formula $\Diamond\Box a$ and there is no LTL formula equivalent to the CTL formula $\forall\Box\exists\Diamond a$.
- For both of CTL and CTL*, path quantifiers can be used: but CTL requires the path quantifiers and the temporal operators to be alternate. In contrast, CTL* does not need to be met such requirement. Note that path quantifiers cannot be applied to the atomic propositions.
- As a result, CTL* strictly subsumes both LTL and CTL. For example, the CTL* formula $\forall\Diamond\Box a$ (which is not legal in CTL) is equivalent to the LTL $\Diamond\Box a$.

3 On Equivalence of CTL and LTL Formulae

Theorem (Thm. 6.18, PMC, p.335)**.** *Let Φ be a CTL formula, and ϕ the LTL formula that is obtained by eliminating all path quantifiers in Φ. Then:*

$$\Phi \equiv \phi \text{ or there does not exist any LTL formula that is equivalent to } \Phi.$$

Example (Handout 15, p.4.)**.** For any CTL formula $\Phi \in \{\forall\Diamond\forall\Box a, \forall\Diamond\exists\Box a, \exists\Diamond\forall\Box a, \exists\Diamond\exists\Box a\}$ and LTL $\phi = \Diamond\Box a$, it is either one of the following cases:

i) $\Phi = \phi$

ii) There does not exist any LTL formula which is equivalent to Φ.

Fact.[Handout 15, p.7.] Let TS and TS' be transition systems such that $\mathsf{Trace}(\mathsf{TS}') \subseteq \mathsf{Trace}(\mathsf{TS})$ and let ϕ be a formula of LTL. Then:

$$\text{If } \mathsf{TS} \models \phi \text{ then } \mathsf{TS'} \models \phi.$$

Theorem (From Thm. 6.21 (b), PMC, p.340)**.** *Consider $\Phi = \forall\Box\exists\Diamond a$, which is a legal CTL formula (hence legal in CTL*). There is no LTL formula ϕ equivalent to Φ.*

That is, there exist CTL formulae for which no equivalent LTL formula exists.

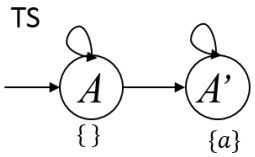
Recall that a CTL formula Φ and a LTL formula ϕ are *equivalent*, denoted $\Phi \equiv \phi$, if for any model or transition system TS, $\mathsf{TS} \models \Phi \iff \mathsf{TS} \models \phi$.

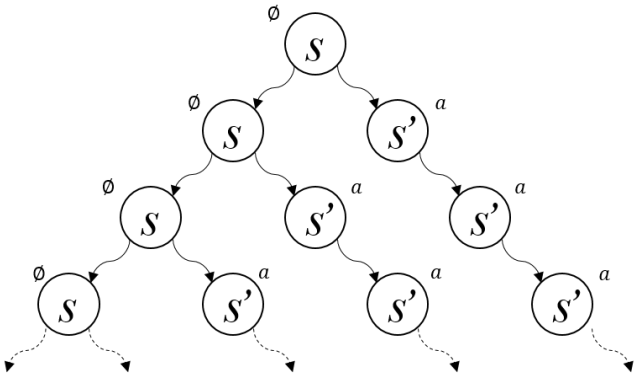
A rule of thumb: Counter-examples are usually simple.

Proof. (by contradiction) For the purpose of contradiction, we assume that there exists an LTL formula ϕ such that

$$\phi \equiv \forall\Box\exists\Diamond a.$$

Now consider a transition system TS depicted in the figure below: It is clear that $\mathsf{TS} \models \forall\Box\exists\Diamond a$(for all

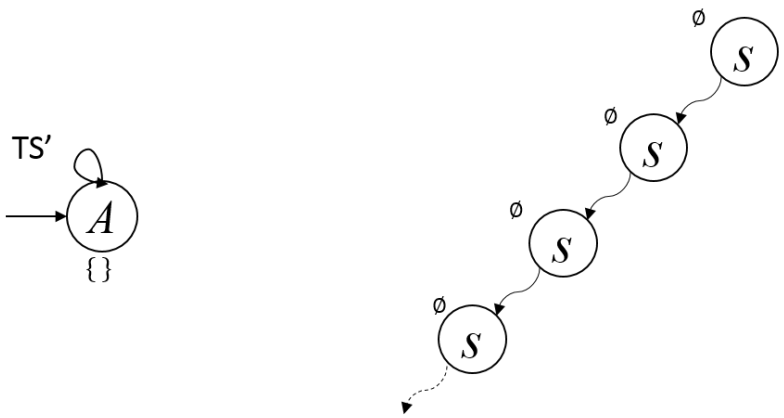




paths, there exists some path eventually a). Then by the assumption,

$$\mathsf{TS} \models \phi.$$

Let TS' be a simple transition system as in the figure below:



Observing that $\mathsf{Path}(\mathsf{TS}') \subset \mathsf{Path}(\mathsf{TS})$, it must be the case that $\mathsf{TS}' \vDash \phi$; but $\mathsf{TS}' \nvDash \Phi$, which contradicts to the assumption $\phi \equiv \Phi$. □

4 What's Next?

So far, we only have seen *propositional* temporal logic. After the spring break, the first-order temporal logic as well as the modal logic will be introduced, and then we will come back to the topics of the model checking such as fairness and complexity of formal verification algorithms.

Propositional logic is a subset of the first order logic. Semantics of the propositional logic is basically the truth table over atomic propositions. The introduction of first order will allow us to deal with more complicated applications. While doing so, we will encounter Hoare logic (HL) and some of its extensions, including relational HL (RHL), probabilistic HL (pHL), and probabilistic relational HL (pRHL), which will be connected to EasyCrypt.

Probabilistic model checking will not be covered[1].

5 Well-Formed Formulas (WFFs) of First Order Logic

- **Signature** of first order logic consists of
  - a set $\mathcal{P}$ of predicate symbols, each of (finite) arity $n \geq 0$,
  - a set $\mathcal{F}$ of function symbols, each of (finite) arity $n \geq 1$, and
  - a set $\mathcal{C}$ of constant symbols, or nullary functions.
- **Terms**[2], in Backus Naur form (BNF), are expressed as

$$t ::= x \mid c \mid f(t, \cdots t)$$

  where x ranges over a set of variables, $c \in \mathcal{C}$ over nullary function symbols, and f over a set of function symbols $\mathcal{F}$.

[1] refer PMC, Ch.10, if interested.
[2] LCS, p.99

- **(Minimal) Syntax of First Order Logic**, in BNF,

$$\varphi ::= P(t_1, \cdots, t_n) \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \exists x \varphi$$

Where $P \in \mathcal{P}$ is a predicate symbol of arity $n \geq 1$, t_i are terms and x is a variable.

Note that $\forall x \varphi \triangleq \neg\exists x \neg\varphi$.