FMSoft
Lecture 2 — Introducing LTL

Tadeusz Litak

October 23, 2018

Informatik 8, FAU Erlangen-Nürnberg

Introducing LTL

- $\phi, \psi ::= \top \mid \mathsf{p} \mid \neg\phi \mid \phi \wedge \psi \mid \mathsf{X}\phi \mid \phi \mathsf{U} \psi$

  Added after the lecture: During the lecture, we went for a more economical syntax w/o $\top$ as primitive, but it is convenient to include
- Semantics defined in terms of paths in models
- Define path truncation as $\pi_n(m) := \pi(n + m)$
- In future, it will be useful to have the following notation

$$\Pi(s) := \{\pi \text{ a path in } \mathcal{M} \text{ s.t. } \pi(0) = s\}$$

LTL **semantics**

- $\mathcal{M}, \pi \vDash \top$: always

  Added after the lecture: We need it if $\top$ is a primitive, otherwise worked out as an exercise: cf. the lecture
- $\mathcal{M}, \pi \vDash \mathsf{p}$ if $\mathsf{p} \in L(\pi(0))$
- $\mathcal{M}, \pi \vDash \neg\phi$ if $\mathcal{M}, \pi \nvDash \phi$
- $\mathcal{M}, \pi \vDash \phi \wedge \psi$ if $\mathcal{M}, \pi \vDash \phi$ and $\mathcal{M}, \pi \vDash \psi$
- $\mathcal{M}, \pi \vDash \mathsf{X}\phi$ if $\mathcal{M}, \pi_1 \vDash \phi$
- $\mathcal{M}, \pi \vDash \phi \mathsf{U} \psi$ if $\exists n \in \mathbb{N}. \mathcal{M}, \pi_n \vDash \psi$ and $\forall i < n. \mathcal{M}, \pi_i \vDash \phi$
- Defined abbreviations: usual booleans plus

$$\mathsf{F}\phi := \top \mathsf{U} \phi \qquad \mathsf{G}\phi := \neg\mathsf{F}(\neg\phi)$$
$$\phi \mathsf{W} \psi := \phi \mathsf{U} \psi \vee \mathsf{G}\phi \qquad \phi \mathsf{R} \psi := \neg(\neg\phi \mathsf{U} \neg\psi)$$

- Exercise: Work out satisfaction clauses for the defined connectives!

- Clause for R may be somewhat non-trivial
- $\mathcal{M}, \pi \vDash \phi \mathsf{R} \psi$ if
  either $\exists n \in \mathbb{N}. \mathcal{M}, \pi_n \vDash \phi$ and $\forall i \leq n. \mathcal{M}, \pi_i \vDash \psi$
  or $\forall n \in \mathbb{N}. \mathcal{M}, \pi_n \vDash \psi$
- ϕ releases ψ. And if ϕ doesn't show up at all, then ψ is not released and has to hold forever ...
- Note also weak inequality

- You may ask yourself …
- …what is $\mathcal{M}$ doing in the satisfaction definition?
- In fact, for LTL we could indeed take a path to be a model in its own right and forget the rest of $\mathcal{M}$
- All that we would need to do is to restrict the domain of the labelling function L from S to π
- However, with CTL and extensions we will not be able to forget about all points not on the present path …
- …so it is just for consistency with the format of other definitions to come

Blackboard examples of paths to be distinguished by LTL formulas …

Equivalences (of path formulas)

- We say that ϕ and ψ are (semantically) equivalent, notation $\phi \equiv \psi$, if for all $\mathcal{M}$ and for all paths π in $\mathcal{M}$

$$\mathcal{M}, \pi \vDash \phi \text{ iff } \mathcal{M}, \pi \vDash \psi$$

- Note this can be stated in terms of defined bi-implication (equivalence connective)
- $\phi \equiv \psi$ if for all $\mathcal{M}$ and for all paths π in $\mathcal{M}$,

$$\mathcal{M}, \pi \vDash \phi \leftrightarrow \psi$$

Exercises

- $\neg \mathsf{F} \phi \equiv \mathsf{G} \neg \phi$
- $\neg \mathsf{X} \phi \equiv \mathsf{X} \neg \phi$
- $\neg (\phi \mathsf{U} \psi) \equiv (\neg \phi \mathsf{R} \neg \psi)$
- $\phi \mathsf{U} \psi \equiv \phi \mathsf{W} \psi \wedge \mathsf{F} \psi$
- $\phi \mathsf{W} \psi \equiv \psi \mathsf{R} (\phi \vee \psi)$
- $\phi \mathsf{R} \psi \equiv \psi \mathsf{W} (\phi \wedge \psi)$

And one more

- $\phi \mathsf{U} \psi \equiv \neg(\neg\psi \mathsf{R} (\neg\phi \wedge \neg\psi)) \wedge \mathsf{F}\psi$

Possible basic sets of connectives

- All these equivalences mean we could make various choices
  if we keep all the booleans of course
- We went for U and X
- But we could also choose R and X
- Or perhaps also W and X
- Clearly, X is orthogonal to all the other connectives
- But also, these equivalences rely on negation bit much …
- What if we want negation-normal form?

NNF definability w/o X

- That is, let us forget X for a while …
- …and also consider the following NNF syntax:
- $\phi, \psi ::= \top \mid \bot \mid \mathsf{p} \mid \neg\mathsf{p} \mid \phi \wedge \psi \mid \phi \vee \psi$
- We focus on F, G, U, R, W
- Which subsets are sufficient in this NNF setting?
- Solution …
- $\{\mathsf{U}, \mathsf{R}\}, \{\mathsf{U}, \mathsf{W}\}, \{\mathsf{U}, \mathsf{G}\}, \{\mathsf{R}, \mathsf{F}\}, \{\mathsf{W}, \mathsf{F}\}$

  Hint: G definable in terms of R when $\bot$ available
- Are there insufficient ones?
- Can you NNF-define F using only $\{\mathsf{R}, \mathsf{G}\}$ or $\{\mathsf{W}, \mathsf{G}\}$?
- Or give such a NNF definition of G using only $\{\mathsf{U}, \mathsf{F}\}$?

Fixpoint(-like) characterizations

- One more important class of equivalences
- This time, they essentially rely on X
- Of course, we cannot define other connectives using X …
- …in a normal way
- but it's different if we allow fixpoint or recursive equations

  remember I told you μ-calculi are particularly powerful?

- $\mathsf{G}\phi \equiv \phi \wedge \mathsf{X}\mathsf{G}\phi$
- $\mathsf{F}\phi \equiv \phi \vee \mathsf{X}\mathsf{F}\phi$
- $\phi \mathsf{U} \psi \equiv \psi \vee (\phi \wedge \mathsf{X}(\phi \mathsf{U} \psi))$

Satisfaction at a state

- Recall: $\mathcal{M}, s \vDash \phi$ if $\forall \pi \in \Pi(s)$, $\mathcal{M}, \pi \vDash \phi$
- Is it the case that $\mathcal{M}, s \vDash \neg\phi$ iff $\mathcal{M}, s \nvDash \phi$ ...?
- Solution: on the blackboard

  (even if a solution is blackboard-only, you still have to be able to produce it during exam!)

Reminder

- Model-checking, however, is not entirely trivial
- One can keep it linear in $|\mathcal{M}|$, i.e., the size of $\mathcal{M}$
- Algorithms, however, tend to blow up in $|\phi|$
- It is possible to design a nondeterministic algorithm running in space polynomial in $|\mathcal{M}|$ and $|\phi|$
- Thus, by Savitch's Theorem, we get a PSPACE model-checking algorithm for LTL
- More to come later

- There are other problems too
- Recall a path formula holds at a state s iff it holds along all paths beginning at s
- How about properties requiring combinations of universal and existential quantifiers over paths available at s and it successors?

- E.g., reachability issues when finding deadlocked states
- In LTL we can say $\mathsf{G}\neg\phi$: *ϕ is false at every reachable state*
- $\mathsf{G}\neg\phi$ is *false* at s iff s can reach some s' s.t. $\mathcal{M}, s' \vDash \phi$
- But how do you say: *every reachable s' can in turn reach (possibly by a different path!)s'' s.t. $\mathcal{M}, s'' \vDash \phi$?*