

FMSoft

Lecture 2 — Introducing LTL

(pre-lecture version)

Tadeusz Litak

October 23, 2018

Informatik 8, FAU Erlangen-Nürnberg

1

Introducing LTL

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

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

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

2

- $\mathcal{M}, \pi \models \top$: always
Added after the lecture: We need it if \top is a primitive, otherwise worked out as an exercise: cf. the lecture
- $\mathcal{M}, \pi \models p$ if $p \in L(\pi(0))$
- $\mathcal{M}, \pi \models \neg\phi$ if $\mathcal{M}, \pi \not\models \phi$
- $\mathcal{M}, \pi \models \phi \wedge \psi$ if $\mathcal{M}, \pi \models \phi$ and $\mathcal{M}, \pi \models \psi$
- $\mathcal{M}, \pi \models X\phi$ if $\mathcal{M}, \pi_1 \models \phi$
- $\mathcal{M}, \pi \models \phi U \psi$ if $\exists n \in \mathbb{N}. \mathcal{M}, \pi_n \models \psi$ and $\forall i < n. \mathcal{M}, \pi_i \models \phi$
- Defined abbreviations: usual booleans plus

$$F\phi := \top U \phi \qquad G\phi := \neg F(\neg\phi)$$

$$\phi W \psi := \phi U \psi \vee G\phi \quad \phi R \psi := \neg(\neg\phi U \neg\psi)$$
- **Exercise:** Work out satisfaction clauses for the defined connectives!

3

- Clause for **R** may be somewhat non-trivial
- $\mathcal{M}, \pi \models \phi R \psi$ if
 either $\exists n \in \mathbb{N}. \mathcal{M}, \pi_n \models \phi$ and $\forall i \leq n. \mathcal{M}, \pi_i \models \psi$
 or $\forall n \in \mathbb{N}. \mathcal{M}, \pi_n \models \psi$
- 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

4

- 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}

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

- 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} ,

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

Exercises

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

And one more

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

9

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**?

10

NNF definability w/o X

- That is, let us forget X for a while ...
- ...and also consider the following **NNF** syntax:
- $\phi, \psi ::= \top \mid \perp \mid \mathbf{p} \mid \neg \mathbf{p} \mid \phi \wedge \psi \mid \phi \vee \psi$
- We focus on **F, G, U, R, W**
- Which subsets are **sufficient** in this NNF setting?
- Solution ...
- $\{\mathbf{U}, \mathbf{R}\}, \{\mathbf{U}, \mathbf{W}\}, \{\mathbf{U}, \mathbf{G}\}, \{\mathbf{R}, \mathbf{F}\}, \{\mathbf{W}, \mathbf{F}\}$
Hint: **G** definable in terms of **R** when \perp available
- Are there insufficient ones?
- Can you NNF-define **F** using only $\{\mathbf{R}, \mathbf{G}\}$ or $\{\mathbf{W}, \mathbf{G}\}$?
- Or give such a NNF definition of **G** using only $\{\mathbf{U}, \mathbf{F}\}$?

11

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?

12

- $G\phi \equiv \phi \wedge XG\phi$
- $F\phi \equiv \phi \vee XF\phi$
- $\phi U \psi \equiv \psi \vee (\phi \wedge X(\phi U \psi))$

Satisfaction at a state

- Recall: $\mathcal{M}, s \models \phi$ if $\forall \pi \in \Pi(s), \mathcal{M}, \pi \models \phi$
- Is it the case that $\mathcal{M}, s \models \neg\phi$ iff $\mathcal{M}, s \not\models \phi$...?
- 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

15

- 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 its successors?

16

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