Formale Spezifikation und Verifikation

Mirco Tribastone

Institut für Informatik
Ludwig-Maximilians-Universität München
tribastone@pst.ifi.lmu.de

Linear-time Temporal Logic

Overview

- Syntax and Semantics of LTL
- Noteworthy Equivalences
- CTL*, CTL, and LTL

Syntax of LTL

Definition

Let Atom be a set of atomic propositions. An LTL formula is given by the following grammar:

$$\phi := \bot \mid \top \mid p \mid (\neg\phi) \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \rightarrow \phi) \mid$$
$$\mathbf{X}\,\phi \mid \mathbf{F}\,\phi \mid \mathbf{G}\,\phi \mid \phi\,\mathbf{U}\,\phi \mid \phi\,\mathbf{W}\,\phi \mid \phi\,\mathbf{R}\,\phi,$$

where $p \in$ Atom is any propositional atom

- **X** stands for *next state*
- **F** stands for *future*
- **G** stands for *globally*
- **U** stands for *until*
- **W** stands for *weak until*
- **R** stands for *release*

Semantics of LTL – 1

Unlike CTL, LTL does not have path quantifiers because the semantics is based on a computation path.

Path

Formally, let $\mathcal{M}$ be a model. A path in $\mathcal{M}$ is an infinite sequence of states $s_1, s_2, \ldots$ such that $s_i \to s_{i+1}$ for all $i \geq 1$.

A path is written $\pi = s_1 \to s_2 \to \ldots$. We write π^i for the suffix starting in state s_i, e.g., $\pi^3 = s_3 \to s_4 \to \ldots$.

In CTL, we had $\mathcal{M}, s \models \phi$ whereas in LTL we have $\mathcal{M}, \pi \models \psi$.

Semantics of LTL – 2

Let $\mathcal{M}$ be a model, $\pi = s_1 \to s_2 \ldots$ be a path, and ϕ an LTL formula. The satisfaction relation $\mathcal{M}, \pi \models \phi$ is defined inductively over the structure of ϕ as follows.

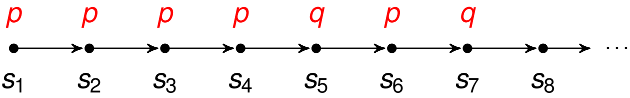
- $\pi \models \top$
- $\pi \not\models \bot$
- $\pi \models p$ iff $p \in L(s_1)$
- $\pi \models \neg\phi$ iff $\pi \not\models \phi$
- $\pi \models \phi_1 \wedge \phi_2$ iff $\pi \models \phi_1$ and $\pi \models \phi_2$
- $\pi \models \phi_1 \vee \phi_2$ iff $\pi \models \phi_1$ or $\pi \models \phi_2$
- $\pi \models \phi_1 \to \phi_2$ iff $\pi \models \phi_2$ whenever $\pi \models \phi_1$

Semantics of LTL – 3

Let $\mathcal{M}$ be a model, $\pi = s_1 \to s_2 \ldots$ be a path, and ϕ an LTL formula. The satisfaction relation $\mathcal{M}, \pi \models \phi$ is defined inductively over the structure of ϕ as follows.

- $\pi \models \mathbf{X}\,\phi$ iff $\pi^2 \models \phi$
- $\pi \models \mathbf{G}\,\phi$ iff $\pi^i \models \phi$, for all $i \geq 1$
- $\pi \models \mathbf{F}\,\phi$ iff there is some $i \geq 1$ such that $\pi^i \models \phi$
- $\pi \models \phi\,\mathbf{U}\,\psi$ iff there is some $i \geq 1$ such that $\pi^i \models \psi$ and $\pi^j \models \phi$ for $j = 1, \ldots, i-1$
- $\pi \models \phi\,\mathbf{W}\,\psi$ iff either there is some $i \geq 1$ such that $\pi^i \models \psi$ and $\pi^j \models \phi$ for $j = 1, \ldots, i-1$; or $\pi^k \models \phi$ for all $k \geq 1$.
- $\pi \models \phi\,\mathbf{R}\,\psi$ iff either there is some $i \geq 1$ such that $\pi^i \models \phi$ and $\pi^j \models \psi$ for $j = 1, \ldots, i$; or for all $k \geq 1$ we have $\pi^k \models \psi$

Pictorial Representation (Temporal Connectives Only)

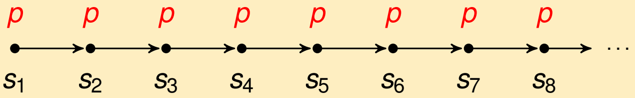


$\pi \models p \,\mathbf{U}\, q$	$\pi \models p \,\mathbf{W}\, q$
$\pi^2 \models p \,\mathbf{U}\, q$	$\pi^2 \models p \,\mathbf{W}\, q$
$\pi^5 \models p \,\mathbf{U}\, q$	$\pi^5 \models p \,\mathbf{W}\, q$
$\pi^8 \not\models p \,\mathbf{U}\, q$	$\pi^8 \not\models p \,\mathbf{W}\, q$

$$\pi \models \phi \,\mathbf{U}\, \psi \implies \pi \models \phi \,\mathbf{W}\, \psi.$$

Pictorial Representation (Temporal Connectives Only)

Weak Until

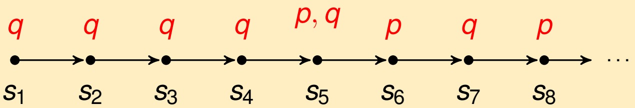


$$\pi \models p\,\mathbf{W}\,q$$

$$\pi \models \mathbf{G}\,p$$

$$\pi \models \mathbf{G}\,p \implies \pi \models p\,\mathbf{W}\,\phi, \qquad \text{for any } \phi.$$

Release

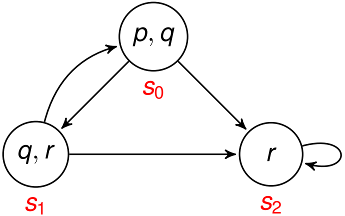


$$\pi \models p\,\mathbf{R}\,q$$

Satisfiability of States

Definition

Let $\mathcal{M} = (S, \rightarrow, L)$ be a model, $s \in S$,and ϕ an LTL formula. We write $\mathcal{M}, s \models \phi$ if, for every execution path π starting from s, we have $\pi \models \phi$.



- $\mathcal{M}, s_0 \models p \wedge q$
- $\mathcal{M}, s_0 \models \neg r$
- $\mathcal{M}, s_0 \models \top$
- $\mathcal{M}, s_0 \models \mathbf{X}\, r$
- $\mathcal{M}, s_0 \not\models \mathbf{X}(q \wedge r)$
- $\mathcal{M}, s_0 \models \mathbf{G}\, \neg(p \wedge r)$
- $\mathcal{M}, s_2 \models \mathbf{F}(\neg q \wedge r)$
- $\mathcal{M}, s_0 \not\models \mathbf{G}\,\mathbf{F}\, p$
- $\mathcal{M}, s_0 \models \mathbf{G}\,\mathbf{F}\, p \rightarrow \mathbf{G}\,\mathbf{F}\, r$

What is the difference between $\mathbf{G}\,\mathbf{F}\, \phi$ and $\mathbf{F}\,\mathbf{G}\, \phi$?

Noteworthy Equivalences

$$\neg\,\mathbf{G}\,\phi \equiv \mathbf{F}\,\neg\phi \qquad \neg\,\mathbf{F}\,\phi \equiv \mathbf{G}\,\neg\phi \qquad \neg\,\mathbf{X}\,\phi \equiv \mathbf{X}\,\neg\phi$$

Proof of $\neg\,\mathbf{G}\,\phi \equiv \mathbf{F}\,\neg\phi$.

Suppose that for some π, $\pi \models \neg\,\mathbf{G}\,\phi$. Thus, $\pi \not\models \mathbf{G}\,\phi$, i.e., there exists some $i \geq 1$ such that $\pi^i \not\models \phi$, that is, $\pi^i \models \neg\phi$, which means $\pi \models \mathbf{F}\,\neg\phi$. Conversely, suppose now that $\pi \models \mathbf{F}\,\neg\phi$. Thus, there exists some $i \geq 1$ such that $\pi^i \models \neg\phi$, i.e. $\pi^i \not\models \phi$. Therefore $\pi \not\models \mathbf{G}\,\phi$, i.e., $\pi \models \neg\,\mathbf{G}\,\phi$. $\square$

$$\neg(\phi\,\mathbf{U}\,\psi) \equiv \neg\phi\,\mathbf{R}\,\neg\psi \qquad \neg(\phi\,\mathbf{R}\,\psi) \equiv \neg\phi\,\mathbf{U}\,\neg\psi$$

$$\mathbf{F}(\phi \vee \psi) \equiv \mathbf{F}(\phi) \vee \mathbf{F}(\psi) \qquad \mathbf{G}(\phi \wedge \psi) \equiv \mathbf{G}(\phi) \wedge \mathbf{G}(\psi)$$

$$\mathbf{F}(\phi \wedge \psi) \equiv \mathbf{F}(\phi) \wedge \mathbf{F}(\psi)\ ?$$

$$\mathbf{F}\,\phi \equiv \top\,\mathbf{U}\,\phi \qquad \mathbf{G}\,\phi \equiv \bot\,\mathbf{R}\,\phi$$

Adequate Set of Connectives

$$\phi\,\mathbf{W}\,\psi \equiv (\phi\,\mathbf{U}\,\psi) \vee \mathbf{G}\,\phi$$
$$\phi\,\mathbf{W}\,\psi \equiv \psi\,\mathbf{R}(\phi \vee \psi)$$
$$\phi\,\mathbf{R}\,\psi \equiv \psi\,\mathbf{W}(\phi \wedge \psi)$$

- The connectives $\vee$, $\rightarrow$ and $\top$ can be expressed in terms of $\perp$, $\wedge$, and $\neg$
- Each of the sets $\{\mathbf{U}, \mathbf{X}\}$, $\{\mathbf{R}, \mathbf{X}\}$, and $\{\mathbf{W}, \mathbf{X}\}$ forms an adequate set of temporal connectives.
- For instance, for $\{\mathbf{U}, \mathbf{X}\}$ we write **R** in terms of **U** with

$$\neg(\phi\,\mathbf{U}\,\psi) \equiv \neg\phi\,\mathbf{R}\,\neg\psi \implies \neg(\neg\phi\,\mathbf{U}\,\neg\psi) \equiv \phi\,\mathbf{R}\,\psi$$

and **W** in terms of **R** (hence, in terms of **U**) using the second equation.

Comparing CTL and LTL: Introduction

Let $\mathcal{M} = (S, \to, L)$ be a model and $s \in S$. The relation

$$\mathcal{M}, s \models \mathbf{F}\, p \to \mathbf{F}\, q$$

is satisfied iff all paths starting from s that have p along them also have q.

Consider now the CTL formula $\mathbf{AF}\, p \to \mathbf{AF}\, q$.
Is it expressing the same property? No, because it says that whenever across all paths starting from s, p is satisfied at some point then across all paths q is satisfied also.

How about the CTL formula $\mathbf{AG}(p \to \mathbf{AF}\, q)$?

Combining CTL and LTL: CTL*

Syntax

- State formulas:

$$\phi := \top \mid p \mid (\neg\phi) \mid (\phi \wedge \phi) \mid \mathbf{A}[\alpha] \mid \mathbf{E}[\alpha]$$

- Path formulas:

$$\alpha := \phi \mid (\neg\alpha) \mid (\alpha \wedge \alpha) \mid \alpha\,\mathbf{U}\,\alpha \mid \mathbf{G}\,\alpha \mid \mathbf{F}\,\alpha \mid \mathbf{X}\,\alpha$$

- LTL as a subset of CTL*: $\mathbf{A}[\alpha]$ ($\mathbf{A}$ means across all paths)
- CTL as a subset of CTL*: we restrict path formulas to

$$\alpha := \alpha\,\mathbf{U}\,\alpha \mid \mathbf{G}\,\alpha \mid \mathbf{F}\,\alpha \mid \mathbf{X}\,\alpha$$

- CTL* formulas that can be expressed neither in LTL nor in CTL, e.g.,

$$\mathbf{E}[\mathbf{G}\,\mathbf{F}\,p]$$

Comparing the Expressive Powers of LTL and CTL

- A formula in CTL but not in LTL: **AG EF** p (across all paths, from any state there exists a path leading to a state where p holds).

Proof.

Suppose toward a contradiction that such an LTL formula exists. It can be written as $\mathbf{A}[\alpha]$, where α is a CTL* path formula.
The model on the left, $\mathcal{M}$, is such that $\mathcal{M}, s \models \mathbf{AG\,EF}\,p$, thus it holds that $\mathcal{M}, s \models \mathbf{A}[\alpha]$.
Now, the paths from s of the model on the right, $\mathcal{M}'$, are a subset of those from the left. Therefore it must hold that $\mathcal{M}', s \models \mathbf{A}[\alpha]$.
However, it is not the case that $\mathcal{M}', s \models \mathbf{AG\,EF}\,p$, a contradiction. $\square$

Comparing the Expressive Powers of LTL and CTL

- A formula in LTL but not in CTL: $\mathbf{A}[\mathbf{G}\,\mathbf{F}\,p \rightarrow q]$ (across all paths, if there are infinitely many p along the path then there is a state labelled with q, i.e., a request made infinitely often is eventually acknowledged).
- A formula in LTL and CTL: $\mathbf{AG}(p \rightarrow \mathbf{AF}\,q)$ in CTL, or $\mathbf{G}(p \rightarrow \mathbf{F}\,q)$ in LTL: across all paths a p is eventually followed by a q.
- However, it is not the case that any LTL formula is always expressible as a CTL formula by prefixing the temporal connectives with $\mathbf{A}$.
  - We saw an example of that with $\mathbf{F}\,p \rightarrow \mathbf{F}\,q$ and $\mathbf{AF}\,p \rightarrow \mathbf{AF}\,q$.