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
- $\text{CTL}^*$, CTL, and LTL
Syntax of LTL

Definition

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

\[ \phi := \bot \mid \top \mid p \mid (\neg \phi) \mid (\phi \land \phi) \mid (\phi \lor \phi) \mid (\phi \rightarrow \phi) \mid X \phi \mid F \phi \mid G \phi \mid \phi U \phi \mid \phi W \phi \mid \phi R \phi, \]

where \( p \in \text{Atom} \) is any propositional atom

- \( \textbf{X} \) stands for \textit{next state}
- \( \textbf{F} \) stands for \textit{future}
- \( \textbf{G} \) stands for \textit{globally}
- \( \textbf{U} \) stands for \textit{until}
- \( \textbf{W} \) stands for \textit{weak until}
- \( \textbf{R} \) stands for \textit{release}
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 $s_i \rightarrow s_{i+1}$ for all $i \geq 1$.

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

In CTL, we had $\mathcal{M}, s \models \phi$ whereas in LTL we have $\mathcal{M}, \pi \models \psi$. 
Let $\mathcal{M}$ be a model, $\pi = s_1 \rightarrow s_2 \ldots$ be a path, and $\phi$ an LTL formula. The satisfaction relation $\mathcal{M}, \pi \models \phi$ is defined inductively over the structure of $\phi$ as follows.

- $\pi \models \top$
- $\pi \not\models \bot$
- $\pi \models p$ iff $p \in L(s_1)$
- $\pi \models \neg \phi$ iff $\pi \not\models \phi$
- $\pi \models \phi_1 \land \phi_2$ iff $\pi \models \phi_1$ and $\pi \models \phi_2$
- $\pi \models \phi_1 \lor \phi_2$ iff $\pi \models \phi_1$ or $\pi \models \phi_2$
- $\pi \models \phi_1 \rightarrow \phi_2$ iff $\pi \models \phi_2$ whenever $\pi \models \phi_1$
Let $M$ be a model, $\pi = s_1 \rightarrow s_2 \ldots$ be a path, and $\phi$ an LTL formula. The satisfaction relation $M, \pi \models \phi$ is defined inductively over the structure of $\phi$ as follows.

- $\pi \models X \phi$ 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 $\pi^k \models \psi$.
\[
\begin{align*}
\pi & \models p \mathbf{U} q \\
\mathbf{p}^2 & \models p \mathbf{U} q \\
\pi^5 & \models p \mathbf{U} q \\
\pi^8 & \not\models p \mathbf{U} q
\end{align*}
\]
\[
\begin{align*}
\pi & \not\models p \mathbf{W} q \\
\mathbf{p}^2 & \models p \mathbf{W} q \\
\pi^5 & \models p \mathbf{W} q \\
\pi^8 & \not\models p \mathbf{W} q
\end{align*}
\]

\[
\begin{align*}
\pi & \models \phi \mathbf{U} \psi \implies \pi \models \phi \mathbf{W} \psi.
\end{align*}
\]
Weak Until

\[ \pi \models p \mathbf{W} q \]
\[ \pi \models \mathbf{G} p \]
\[ \pi \models \mathbf{G} p \implies \pi \models p \mathbf{W} \phi, \text{ for any } \phi. \]

Release

\[ \pi \models p \mathbf{R} q \]
Satisfiability of States

Definition

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

- \( \mathcal{M}, s_0 \models p \land q \)
- \( \mathcal{M}, s_0 \models \neg r \)
- \( \mathcal{M}, s_0 \models \top \)
- \( \mathcal{M}, s_0 \not\models X(r \land q) \)
- \( \mathcal{M}, s_0 \models G \neg(p \land r) \)
- \( \mathcal{M}, s_0 \not\models GFp \)
- \( \mathcal{M}, s_0 \models G \neg(p \land r) \rightarrow GFr \)

What is the difference between \( GF\phi \) and \( FG\phi \)?
Noteworthy Equivalences

\[ \neg G \phi \equiv F \neg \phi \quad \neg F \phi \equiv G \neg \phi \quad \neg X \phi \equiv X \neg \phi \]

Proof of \( \neg G \phi \equiv F \neg \phi \).

Suppose that for some \( \pi \), \( \pi \models \neg G \phi \). Thus, \( \pi \not\models G \phi \), i.e., there exists some \( i \geq 1 \) such that \( \pi^i \not\models \phi \), that is, \( \pi^i \models \neg \phi \), which means \( \pi \models F \neg \phi \).

Conversely, suppose now that \( \pi \models F \neg \phi \). Thus, there exists some \( i \geq 1 \) such that \( \pi^i \models \neg \phi \), i.e. \( \pi^i \not\models \phi \). Therefore \( \pi \not\models G \phi \), i.e., \( \pi \models \neg G \phi \). \( \square \)

\[ \neg (\phi U \psi) \equiv \neg \phi R \neg \psi \quad \neg (\phi R \psi) \equiv \neg \phi U \neg \psi \]

\[ F(\phi \lor \psi) \equiv F(\phi) \lor F(\psi) \quad G(\phi \land \psi) \equiv G(\phi) \land G(\psi) \]

\[ F(\phi \land \psi) \equiv F(\phi) \land F(\psi) \ ? \]

\[ F \phi \equiv \top U \phi \quad G \phi \equiv \bot R \phi \]
Adequate Set of Connectives

\[ \phi W \psi \equiv (\phi U \psi) \lor G \phi \]
\[ \phi W \psi \equiv \psi R(\phi \lor \psi) \]
\[ \phi R \psi \equiv \psi W(\phi \land \psi) \]

- The connectives \( \lor, \rightarrow \) and \( \top \) can be expressed in terms of \( \bot, \land, \) and \( \neg \)
- Each of the sets \( \{U, X\}, \{R, X\}, \) and \( \{W, X\} \) forms an adequate set of temporal connectives.
- For instance, for \( \{U, X\} \) we write \( R \) in terms of \( U \) with

\[ \neg(\phi U \psi) \equiv \neg \phi R \neg \psi \implies \neg(\neg \phi U \neg \psi) \equiv \phi R \psi \]

and \( W \) in terms of \( R \) (hence, in terms of \( U \)) using the second equation.
Let $\mathcal{M} = (S, \rightarrow, L)$ be a model and $s \in S$. The relation

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

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

Consider now the CTL formula $\mathbf{AF} p \rightarrow \mathbf{AF} q$. 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 $\mathbf{AG}(p \rightarrow \mathbf{AF} q)$?
Combining CTL and LTL: CTL*

Syntax

- **State formulas:**
  \[ \phi ::= \top \mid p \mid (\neg \phi) \mid (\phi \land \phi) \mid A[\alpha] \mid E[\alpha] \]

- **Path formulas:**
  \[ \alpha ::= \phi \mid (\neg \alpha) \mid (\alpha \land \alpha) \mid \alpha U \alpha \mid G \alpha \mid F \alpha \mid X \alpha \]

- **LTL as a subset of CTL**: \( A[\alpha] \) (\( A \) means across all paths)

- **CTL as a subset of CTL**: we restrict path formulas to
  \( \alpha ::= \alpha U \alpha \mid G \alpha \mid F \alpha \mid X \alpha \)

- **CTL** formulas that can be expressed neither in LTL nor in CTL, e.g.,
  \( E[G F p] \)
A formula in CTL but not in LTL: \( \text{AG EF } p \) (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 \( \text{A}[\alpha] \), where \( \alpha \) is a CTL\(^*\) path formula. The model on the left, \( \mathcal{M} \), is such that \( \mathcal{M}, s \models \text{AG EF } p \), thus it holds that \( \mathcal{M}, s \models \text{A}[\alpha] \).

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 \( \mathcal{M}', s \models \text{A}[\alpha] \).

However, it is not the case that \( \mathcal{M}', s \models \text{AG EF } p \), a contradiction. \( \square \)
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 $\mathbf{AF} p \rightarrow \mathbf{AF} q$. 