Linear Temporal Logic

Presented by

Kevin Browne
Fei Zhao

November 19, 2007
Introduction to Temporal Logic

Why Temporal Logic?
- Formulae statically true or false for a given model in classical propositional, predicate logic
- Most systems are dynamic
- Property verification for concurrent, reactive systems

Temporal Logic
- Formulae are not statically true or false in a model
- Models are transitions systems
- Dynamic notion of truth
Linear Temporal Logic

- Timeline is the underlying structure of time in Linear Temporal Logic
- We assume time in LTL is isomorphic to the natural numbers
- Under this assumption, time in LTL:
  ◦ Is discrete
  ◦ Has an initial moment with no predecessors
  ◦ Is infinite into the future
- Timeline is a set of paths: $t_0 \ t_1 \ t_2 \ ...$
Linear vs. Branching

- **Linear-time Temporal Logic**
  - Time as a set of paths
  - Each path is a sequence of moments
  - At each moment, only one possible next future moment

- **Computational Tree Logic (Branching)**
  - Time as a tree
  - Root as present moment
  - Branches out into the future
Linear vs. Branching (Intuition)

(Alessandro Artable, “Formal Methods”)
Syntax

The rules for generating Linear Temporal Logic (LTL):

- Each $\varphi$ is a formula
- If $\varphi$ and $\psi$ are formulae then $\neg \varphi$, $\varphi \land \psi$, $\varphi \lor \psi$, $\varphi \rightarrow \psi$ are formulae
- If $\varphi$ and $\psi$ are formulae then $X \varphi$, $F \varphi$, $G \varphi$, $\varphi U \psi$, $\varphi W \psi$, $\varphi R \psi$
Syntax (cont’d)

Defined in Backus Naur Form:

\[ \varphi ::= p \mid \text{True} \mid \text{False} \]
\[ \mid \neg \varphi \mid \varphi \land \psi \mid \varphi \lor \psi \mid \varphi \rightarrow \psi \]
\[ \mid X \varphi \mid F \varphi \mid G \varphi \mid U \psi \mid W \psi \mid R \psi \]

Atomic propositions: \( p \in \text{Atoms} \)
Boolean operators: \( \land \lor \neg \rightarrow \)
Temporal operators: \( X \ G \ F \ U \ W \ R \)
Well Formed Formulae

The well formed formulae in LTL follow the same rules as well formed formulae in classical propositional logic, plus the rules for temporal operators.

The following are **NOT** well formed formulae:

- **U** r – since **U** is a binary operator, not unary
- p **G** q – since **G** is a unary operator, not binary
Syntax Examples

- \( \text{F} \ p \land \text{G} \ q \rightarrow p \ \text{W} \ r \)
- \( \text{F} \ (p \rightarrow \text{G} \ r) \lor \neg \ q \ \text{U} \ p \)
- \( p \ \text{W} \ (q \ \text{W} \ r) \)
- \( \text{G} \ \text{F} \ p \rightarrow \text{F}(q \lor s) \)
More Practical Syntax Examples

- \(((x = 0) \land (x + 3)) \rightarrow X \ (x = 3)\)
- lottery-win \rightarrow G rich
- send \rightarrow F receive
- start-lecture \rightarrow talk U end-lecture
- born \rightarrow alive U dead
Transition System

Timeline as a linear time structure $M=\langle S, \rightarrow, L \rangle$ where

- $S$ is a set of states,
- $\rightarrow$ is a transition relation such that every $s \in S$ has some $r \in S$ with $s \rightarrow r$
- $L : S \rightarrow \text{PowerSet (Atoms)}$ is a labeling of each state with a set of atomic propositions in Atoms.

Semantics are given with respect to a path $\pi = s_1 s_2 s_3 \ldots$

Suffix of trace starting at $s_i$ is defined as $\pi_i = s_i s_{i+1} s_{i+2} \ldots$
Transition System Example

\[ M = (S, \rightarrow, L) \] is as follows:

\[ S = \{S_1, S_2, S_3\} \]

\[ \rightarrow = \{(S_1, S_1), (S_1, S_3), (S_1, S_2), (S_2, S_3), (S_3, S_2)\} \]

\[ L(S_1) = \{p, q\} \]
\[ L(S_2) = \{p, r\} \]
\[ L(S_3) = \{q, r\} \]
The set of paths is limited by what we can construct from the given states and transitions. So

\[ \pi = S_1, S_1, S_1, S_1, S_1, S_1, S_1, \ldots \]

and

\[ \pi = S_1, S_1, S_3, S_2, S_3, S_2, \ldots \]

are in \( M \) (read: can be defined by it). But

\[ \pi = S_1, S_1, S_3, S_2, S_1, S_1, \ldots \]

is not!
Semantics

- $\pi | = \text{ True}$
- $\text{not } \pi | = \text{ False}$
- $\pi | = p \iff p \in L(s_1) \ (\pi = s_1 s_2 s_2 \ldots)$
- $\pi | = \neg \varphi \iff \text{not } \pi | = \varphi$
- $\pi | = \varphi \land \psi \iff \pi | = \varphi \text{ and } \pi | = \psi$
- $\pi | = \varphi \lor \psi \iff \pi | = \varphi \text{ or } \pi | = \psi$
- $\pi | = \varphi \rightarrow \psi \iff \pi | = \varphi \text{ if } \pi | = \psi$
- $\pi | = X \varphi \iff \pi_2 | = \varphi$
  (holds iff $\varphi$ holds at the next state)
- $\pi | = F \varphi \iff \exists i \geq 1 \pi_i | = \varphi$
  (at some future state $\varphi$ is true)
Semantics (cont’d)

- $\pi \models G \varphi$ iff $\forall i \geq 1 \pi_i \models \varphi$
  (at all the future states, $\varphi$ is true)

- $\pi \models \varphi U \psi$ iff $\exists i \geq 1 \pi_i \models \psi$ and $\forall j < i \pi_j \models \varphi$
  ($\varphi$ is true until $\psi$ is true)

- $\pi \models \varphi W \psi$ iff ($\exists i \geq 1 \pi_i \models \psi$ and $\forall j < i \pi_j \models \varphi$)
  or $\forall k \geq 1 \pi_k \models \varphi$
  ($\varphi$ is true until $\psi$ is true, or $\varphi$ is always true)

- $\pi \models \varphi R \psi$ iff ($\exists i \geq 1 \pi_i \models \varphi$ and $\forall j < i \pi_j \models \psi$)
  or $\forall k \geq 1 \pi_k \models \psi$
  ($\psi$ is true until $\varphi$ is true, or $\psi$ is always true)
Semantics (Intuition)

\[ S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_5 \rightarrow S_6 \rightarrow S_7 \rightarrow \ldots \]

\[ p \quad U \quad q \quad (p \text{ until } q) \]

\[ S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_5 \rightarrow S_6 \rightarrow S_7 \rightarrow \ldots \]

\[ p \quad W \quad q \quad (p \text{ weak until } q) \]

\[ S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_5 \rightarrow S_6 \rightarrow S_7 \rightarrow \ldots \]

\[ q \quad R \quad p \quad (p \text{ release } q) \]
From this model, we can derive different (infinite) paths:

\[ \pi = S_1, S_1, S_1, S_1, S_1, S_1, S_1, \ldots \]

\[ \pi = S_1, S_1, S_2, S_3, S_2, S_3, \ldots \]

\[ \pi = S_1, S_1, S_3, S_2, S_3, S_2, \ldots \]
Given a path \( \pi \), and a formula \( \varphi \), we can now evaluate the truth of that formula.

So for:

\[ \pi = S1,S1,S1,S1,S1,S1,S1,\ldots \]

\( \pi \models p \) is true

by the rule that “\( \pi \models p \) iff \( p \in L(s_1) \)”. 

Semantic Notion Applied (Cont’d)
Semantics Example

Given the model to the left, we can then say for
\( \pi = S1, S1, S3, S2, S3, S2, S3, \ldots \)

\[ \pi \models p \text{ is true} \]
\[ \pi \models q \text{ is true} \]
\[ \pi \models p \land q \text{ is true} \]
\[ \pi \models r \text{ is false} \]
\[ \pi \models Fp \text{ is true} \]
\[ \pi \models Xp \text{ is true} \]
\[ \pi \models X(Xp) \text{ is false} \]
\[ \pi \models Gr \text{ is false} \]
\[ \pi \models G(X(Xr)) \text{ is true} \]
\[ \pi \models pU\ r \text{ is true} \]
Another Semantics Example

Given the model to the left, we can then say for
\( \pi = S1,S1,S3,S2,S2,\ldots \)

\( \pi \models p \) is true
\( \pi \models X p \) is true
\( \pi \models X (X p) \) is false
\( \pi \models p U r \) is false
\( \pi \models q U r \) is true
\( \pi \models q W r \) is true
\( \pi \models r R q \) is true
\( \pi \models F p \) is true
\( \pi \models F (X (X p)) \) is false
Same Model, Different Paths

Given the model to the left, we can then say for

\[ \pi = S1,S1,S3,S2,S2,\ldots \]

\[ \pi \models p \cup r \] is **FALSE**

But for:

\[ \pi = S1,S2,S2,S2,\ldots \]

\[ \pi \models p \cup r \] is **TRUE**

Truth is no longer static for a given model.
Different paths may evaluate differently for the same formula!
Further Definitions

**Entailment:** \( f \models y \) iff \( \forall M, \forall i \in \mathbb{N}. (M, \pi_i) \models f \Rightarrow (M, \pi_i) \models y \)

**Equivalence:** \( f \equiv y \) iff \( \forall M, \forall i \in \mathbb{N}. (M, \pi_i) \models f \Leftrightarrow (M, \pi_i) \models y \)

**Satisfiable:** An LTL formula \( \varphi \) is satisfiable iff there exists a linear time structure \( M = (S, \rightarrow, L) \) such that \( M, \pi \models \varphi \). Any such structure defines a model of \( \varphi \).

**Valid:** A formula \( \varphi \) is valid iff for all linear time structures \( M = (S, \rightarrow, L) \), we have \( M, \pi \models \varphi \), and write \( \models \varphi \).
Examples:

Some significant validities
- \( |= \mathbf{G} \neg p \equiv \neg \mathbf{F} p \)
- \( |= \mathbf{F} \neg p \equiv \neg \mathbf{G} p \)
- \( |= \mathbf{X} \neg p \equiv \neg \mathbf{X} p \)

Satisfiable or valid
- \( p \rightarrow \mathbf{F} q \)
  - satisfiable formula but not valid
- \( \mathbf{G} (p \rightarrow \mathbf{F} q) \rightarrow (p \rightarrow \mathbf{F} q) \)
  - valid formula
Conclusion

- Linear Temporal Logic is a useful and accessible framework for modeling systems which involve changes occurring over time!

- Questions?
Bibliography

Logic in Computer Science, Michael Huth and Mark Ryan

Handbook of Theoretical Computer Science (Temporal and Modal Logic, Ch. 16), E. Allen Emerson

Formal Methods (Lecture 3: Linear Temporal Logic), Allesandro Artale