Model Checking: Linear-Time Temporal Logic (LTL)

Assaf Kfoury

March 25, 2015 (modified March 31, 2015)
model checking is based on temporal logic

- a model $\mathcal{M}$ of temporal logic contain several **states**
- $\mathcal{M}$ is a **transition system**
- a property $\varphi$ to be checked about $\mathcal{M}$ is a WFF in temporal logic
- $\varphi$ can be true in some states and false in other states of $\mathcal{M}$

- truth in temporal logic is **dynamically** defined
- in contrast to propositional, first-order, and second-order logics, where the truth of WFF’s is **statically** defined

- many different temporal logics, depending on the “structure” of time
  - **linear time** – time is a single execution path, a line
  - **branching time** – time is a tree, rooted at present moment and branching into the future
  - **discrete time**
  - **continuous time**
linear-time temporal logic (LTL)

▶ syntax of LTL

\[ \varphi, \psi ::= \top | \bot | p | \neg \varphi | \varphi \land \psi | \varphi \lor \psi | \varphi \rightarrow \psi \]  

propositional logic

| X\varphi     | “next” state |
| F\varphi    | some “future” state |
| G\varphi    | all “future” states (“globally”) |
| \varphi U \psi | “until” |
| \varphi W \psi | “weak until” |
| \varphi R \psi | “release” |

▶ unary connectives bind most tightly

▶ binary temporal connectives \{U, W, R\} bind more tightly than \{\land, \lor, \rightarrow\}

▶ binary logical connectives \{\land, \lor\} bind more tightly than \{\rightarrow\}
semantics of LTL

- a model $M$ of LTL is a **transition system**, $M \triangleq (S, \rightarrow, L)$ where
  
  $S$ is a set of **states**,
  
  $\rightarrow$ is a binary relation on $S$ such that
  
  for every $s \in S$ there is $s'$ such that $s \rightarrow s'$,  

  $L$ is a **labelling function** $L : S \rightarrow \mathcal{P}($atoms$)$.

- a **path** $\pi$ in $M$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \rightarrow s_2, s_2 \rightarrow s_3, s_3 \rightarrow s_4, \ldots$ we also write

  $\pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$

- for every $i \geq 1$, $\pi^i$ is the suffix of $\pi$ starting at $s_i$, i.e.,

  $\pi^i \triangleq s_i \rightarrow s_{i+1} \rightarrow s_{i+2} \rightarrow \cdots$
semantics of LTL [LCS, page 180, Definition 3.6]

- satisfaction of a WFF of LTL is defined relative to a path

\[ \pi \triangleq s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots \] in a transition system \( \mathcal{M} \triangleq (S, \rightarrow, L) \)

1. \( \pi \models \top \)
2. \( \pi \models \bot \)
3. \( \pi \models p \) \iff \( p \in L(s_1) \)
4. \( \pi \models \neg \varphi \) \iff \( \pi \not\models \varphi \)
5. \( \pi \models \varphi \land \psi \) \iff \( \pi \models \varphi \) and \( \pi \models \psi \)
6. \( \pi \models \varphi \lor \psi \) \iff \( \pi \models \varphi \) or \( \pi \models \psi \)
7. \( \pi \models \varphi \rightarrow \psi \) \iff \( \pi \models \psi \) whenever \( \pi \models \varphi \)
8. \( \pi \models X\varphi \) iff \( \pi^2 \models \varphi \)

9. \( \pi \models G\varphi \) iff for every \( i \geq 1 \) \( \pi^i \models \varphi \)

10. \( \pi \models F\varphi \) iff there is \( i \geq 1 \) \( \pi^i \models \varphi \)
11. \( \pi \models \varphi U \psi \) iff there is \( i \geq 1 \) such \( \pi^i \models \psi \) and 
\[ \pi^1 \models \varphi, \pi^2 \models \varphi, \ldots, \pi^{i-1} \models \varphi \]

12. \( \pi \models \varphi W \psi \) iff \textbf{EITHER} there is \( i \geq 1 \) such \( \pi^i \models \psi \) and 
\[ \pi^1 \models \varphi, \pi^2 \models \varphi, \ldots, \pi^{i-1} \models \varphi \]
\textbf{OR} for every \( k \geq 1 \) we have \( \pi^k \models \varphi \)

13. \( \pi \models \varphi R \psi \) iff \textbf{EITHER} there is \( i \geq 1 \) such \( \pi^i \models \varphi \) and 
\[ \pi^1 \models \psi, \pi^2 \models \psi, \ldots, \pi^i \models \psi \]
\textbf{OR} for every \( k \geq 1 \) we have \( \pi^k \models \psi \)
semantics of LTL [LCS, page 182, Definition 3.8]

- we extend satisfaction of a WFF $\varphi$ of LTL relative to a state $s \in S$ in a transition system $\mathcal{M} \triangleq (S, \rightarrow, L)$

- we write

$$\mathcal{M}, s \models \varphi$$

or if $\mathcal{M}$ is clear from the context, we write

$$s \models \varphi$$

iff **for every path $\pi$ that starts at $s$ we have** $\pi \models \varphi$

- test your understanding of the semantics of LTL with the examples 1 to 10 right after Definition 3.8, page 182
practical patterns of specifications with LTL [LCS,Sect. 3.2.3]

- $\varphi \triangleq \mathbf{G}(\text{started } \rightarrow \text{ready})$
  
  if $\pi \models \varphi$, then in every state along $\pi$, “ready” is true whenever “started” is true

- $\varphi \triangleq \mathbf{G}(\text{requested } \rightarrow \mathbf{F} \text{ acknowledged})$
  
  if $\pi \models \varphi$, then in every state along $\pi$, if a “request” (of some resource) occurs, it will eventually be “acknowledged”

- $\varphi \triangleq \mathbf{G} \mathbf{F} \text{ enabled}$
  
  if $\pi \models \varphi$, then $\pi$ makes “enabled” true infinitely often

- $\varphi \triangleq \mathbf{F} \mathbf{G} \text{ deadlock}$
  
  if $\pi \models \varphi$, then $\pi$ will eventually make “deadlock” continuously true

- $\varphi \triangleq \mathbf{G} \mathbf{F} \text{ enabled } \rightarrow \mathbf{G} \mathbf{F} \text{ running}$
  
  if $\pi \models \varphi$, then if “enabled” occurs infinitely often along $\pi$, then “running” occurs infinitely often along $\pi$

- not every temporal assertion is expressible in LTL, e.g., the following is not

  for every state $s$, there is a path from $s$ that enters a state $s'$ where “restart” is true
practical patterns of specifications with LTL (not in [LCS])

\[ \varphi \triangleq G \neg (\text{read} \land \text{write}) \]

if \( \pi \models \varphi \), then in every state along \( \pi \), not both “read” and “write” are simultaneously true

\[ \varphi \triangleq G(\text{requested} \rightarrow (\text{requested} U \text{ granted})) \]

if \( \pi \models \varphi \), then in every state along \( \pi \), if a “request” (of some resource) occurs, then the “request” will persist in every subsequent state until it is “granted”
equivalence between LTL formulas, [LCS, pp 184-186]

- **definition**: formulas $\varphi$ and $\psi$ are equivalent, $\varphi \equiv \psi$, iff for every model (transition system) $M$ and every path $\pi$ in $M$, we have $\pi \models \varphi$ iff $\pi \models \psi$

- Dualities in LTL:
  - $\neg G \varphi \equiv F \neg \varphi$
  - $\neg F \varphi \equiv G \neg \varphi$
  - $\neg X \varphi \equiv X \neg \varphi$
  - $\neg (\varphi U \psi) \equiv \neg \varphi R \neg \psi$
  - $\neg (\varphi R \psi) \equiv \neg \varphi U \neg \psi$

- For a rigorous proof (at the meta-level) of the last equivalence: go to page 16. Rigorous proofs for all other equivalences are similar.
equivalence between LTL formulas, [LCS, pp 184-186]

- Distributive Laws in LTL:

- $X (\varphi \lor \psi) \equiv X \varphi \lor X \psi$

- $X (\varphi \land \psi) \equiv X \varphi \land X \psi$

- $X (\varphi U \psi) \equiv (X \varphi) U (X \psi)$

- $F (\varphi \lor \psi) \equiv F \varphi \lor F \psi$

- $G (\varphi \land \psi) \equiv G \varphi \land G \psi$

- $\varphi U (\psi_1 \lor \psi_2) \equiv (\varphi U \psi_1) \lor (\varphi U \psi_2)$

- $(\varphi_1 \land \varphi_2) U \psi \equiv (\varphi_1 U \psi) \land (\varphi_2 U \psi)$
equivalence between LTL formulas, [LCS, pp 184-186]

- Inter-Definitions in LTL:
  - $F \varphi \equiv \neg G \neg \varphi$
  - $G \varphi \equiv \neg F \neg \varphi$
  - $F \varphi \equiv \top U \varphi$
  - $G \varphi \equiv \bot R \varphi$
  - $\varphi U \psi \equiv \varphi W \psi \land F \psi$
  - $\varphi W \psi \equiv \varphi U \psi \lor G \varphi$
equivalence between LTL formulas

- **Idempotency Laws in LTL:**
  - $F F \varphi \equiv F \varphi$
  - $G G \varphi \equiv G \varphi$
  - $\varphi U \psi \equiv \varphi U (\varphi U \psi)$

- **Some (perhaps surprising) equivalences in LTL:**
  - $G F G \varphi \equiv F G \varphi$
  - $F G F \varphi \equiv G F \varphi$
  - $G (F \varphi \lor F \psi) \equiv G F \varphi \lor G F \psi$
equivalence between LTL formulas

- although $F$ has similarities with $\exists$, $F$ does not distribute over $\land$

- there is a model $M$ that distinguishes $F(\varphi \land \psi)$ from $(F\varphi \land F\psi)$ for some $\varphi$ and $\psi$
meta-level (and rigorous) proof of an equivalence:

To prove the equivalence $\neg(\varphi \mathcal{R} \psi) \equiv \neg \varphi \mathcal{U} \neg \psi$ we need to show:

for every path $\pi$ 
\[
\left( \pi \models \neg(\varphi \mathcal{R} \psi) \quad \text{iff} \quad \pi \models \neg \varphi \mathcal{U} \neg \psi \right)
\]

Equivalently, we need to show:

for every path $\pi$ 
\[
\left( \pi \models \varphi \mathcal{R} \psi \quad \text{iff} \quad \pi \models \neg(\neg \varphi \mathcal{U} \neg \psi) \right)
\]

What follows in the succeeding pages is a proof of this equivalence:

- It is a meta-level proof, not a formal proof, because we do not use a natural deduction system, or some other formal proof system for LTL. This meta-level proof uses the formal semantics of LTL (defined here).

- We can set up a natural deduction system, and establish its soundness and completeness relative to the formal semantics of LTL, from which our meta-level proof will imply the existence of a formal proof. However, such a natural deduction system for LTL is beyond the scope of CS 512.

- Nevertheless, for the sake of rigor, we use formal logical notation as much as possible in our meta-level proof.
meta-level (and rigorous) proof of an equivalence:

For an arbitrarily given path $\pi$, we have the following sequence of equivalences:

1. $\pi \models \neg(\neg \varphi \mathbf{U} \neg \psi)$  
   (by the definition of $\mathbf{U}$)

2. $\neg(\exists j \geq 1) \left( \pi^i \models \neg \psi \land (\forall i < j) (\pi^i \models \neg \varphi) \right)$  
   (by the semantics of $\neg$)

3. $\neg(\exists j \geq 1) \left( \pi^i \not\models \psi \land (\forall i < j) (\pi^i \not\models \varphi) \right)$  
   (by the duality of $\exists$ and $\forall$)

4. $\forall j \geq 1 \neg \left( \pi^i \not\models \psi \land (\forall i < j) (\pi^i \not\models \varphi) \right)$  
   (by de Morgan’s law)

5. $\forall j \geq 1 \left( \neg(\pi^j \not\models \psi) \lor \neg(\forall i < j) (\pi^i \not\models \varphi) \right)$  
   (by the semantics of $\neg$ and the duality of $\exists$ and $\forall$)

6. $\forall j \geq 1 \left( \pi^i \models \psi \lor (\exists i < j) (\pi^i \models \varphi) \right)$
meta-level (and rigorous) proof of an equivalence:

(6) \((\forall j \geq 1) \left( \pi^j \models \psi \lor (\exists i < j) (\pi^i \models \varphi) \right)\) \iff (by the duality of (non-intuitionistic) \(\rightarrow\) and \(\lor\))

(7) \((\forall j \geq 1) \left( \pi^j \not\models \psi \rightarrow (\exists i < j) (\pi^i \models \varphi) \right)\) \iff (by a re-arrangement of subexpressions)

(8) \((\forall j \geq 1) (\pi^j \models \psi)\) (8.1)

or \((\exists i \geq 1) \left( \pi^i \models \varphi \land (\forall k \leq i)(\pi^k \models \psi) \right)\) (8.2)

All the preceding equivalences, from (1) to (7), are straightforward. The one which needs further justification is (8) = ((8.1) or (8.2)). We consider two possibilities for the path \(\pi\):

(a) **Either** for every \(j \geq 1\), we have \(\pi^j \models \psi\), in which case both (7) and (8.1) hold – or, which is easier to see, both (6) and (8.1) hold. Hence, (6), (7) and (8) hold.

(b) **Or** there are \(1 \leq j_0 < j_1 < j_2 < \cdots\) such that \(\pi^{j_0} \not\models \psi\), \(\pi^{j_1} \not\models \psi\), \(\pi^{j_2} \not\models \psi\), \ldots and for all \(k \not\in \{j_0, j_1, j_2, \ldots\}\), we have \(\pi^k \models \psi\). Hence, if (7) holds, there is \(i < j_0\) such that \(\pi^i \models \varphi\) and for all \(k \leq i < j_0\), it holds that \(\pi^k \models \psi\), thus implying (8.2). Conversely, if (8.2) holds, then (7) holds. Hence, (7) iff (8).

Hence, whether (a) or (b) is the case, we have (7) iff (8).
meta-level (and rigorous) proof of an equivalence:

A closer look at (8) shows that:

\[\forall j \geq 1 (\pi^j \models \psi) \text{ or } \exists i \geq 1 (\pi^i \models \varphi \land (\forall k \leq i)(\pi^k \models \psi))\]

is a more formal re-wording of the semantics of $R$ (defined [here](#)). Hence, (8) holds iff:

\[\pi \models \varphi R \psi\]

Since $\pi$ is an arbitrarily given path, we conclude that for every path $\pi$, we have (1) iff (9). This completes our meta-level rigorous proof.