SLR 204: Basics of verification of distributed systems

Vadim Malvone
vadim.malvone@telecom-paris.fr
Formal Specification of Properties in Linear-time Temporal Logic (LTL)
LTL: Linear-time Temporal Logic (I)

- It determines patterns on infinite traces.
- At any time, there can be only one future.
- Elements:
  - Atomic propositions: AP
  - Boolean operators: \(\neg\) (NOT), \(\lor\) (OR), \(\land\) (AND)
  - Temporal operators:
    - \(X\) (NEXT)
    - \(F\) (EVENTUALLY)
    - \(G\) (GLOBALLY)
    - \(U\) (UNTIL)
LTL: Linear-Time Temporal-Logic (II)

$p$ “$p$ is true now”
LTL: Linear-Time Temporal-Logic (III)

\[ X p \quad \text{“p has to hold at the next state”} \]

\[ s_0 \quad s_1 \quad s_2 \quad s_3 \]

- \[ s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \] (False)
- \[ \neg p \rightarrow p \rightarrow \neg p \rightarrow \neg p \] (False)
- \[ s_0 \rightarrow p \rightarrow s_2 \rightarrow s_3 \] (True)
LTL: Linear-Time Temporal-Logic (IV)

F p  “p has to hold sooner or later”

- F(p ∨ q) is equivalent to Fp ∨ Fq

¬Fp  “p is false now and is never verified in the future”
LTL: Linear-Time Temporal-Logic (V)

\( Gp \) “p has to hold globally”

- \( Gp \) is equivalent to \( \neg F \neg p \)
- \( G(p \land q) \) is equivalent to \( Gp \land Gq \)
LTL: Linear-Time Temporal-Logic (VI)

\[ p \mathbf{U} q \]  
“p has to hold at least until q becomes true”
Example

Does the following execution satisfy $X (p \cup (q \land F r))$?

$p U (q \land F r)$

$q \land F r$

$F r$

$r$

$X (p U (q \land F r))$
Formal Syntax of LTL (I)

\[ \psi : = p \mid \neg \psi \mid \psi \lor \psi \mid X \psi \mid \psi U \psi \]

where \( p \in AP \)

- LTL formulas are evaluated on infinite paths.
- An LTL formula describes a set of paths for which the formula holds.
- Given a model \( M \), a path starting in a state \( s_0 \in S_0 \) is an infinite sequence \( \pi = s_0s_1s_2s_3 ... \) such that \( \forall i \geq 0, R(s_i, s_{i+1}) \).
Formal Syntax of LTL (II)

- **Derived operators:**
  - $true = p \lor \neg p$
  - $F\psi = true \lor \psi$
  - $G\psi = \neg F\neg \psi$

- **Some rewriting (step unfolding) rules:**
  - $F\psi = \psi \lor XF\psi$
  - $G\psi = \psi \land XG\psi$
  - $\psi_1 U \psi_2 = \psi_2 \lor (\psi_1 \land X (\psi_1 U \psi_2))$
Formal Semantics of LTL (I)

- Given $M = (AP, S, S_0, R, Lab)$ and $\pi = s_0s_1s_2s_3 \ldots$, where $s_0 \in S_0$

- $\pi \models \psi$ means that the LTL formula $\psi$ holds on $\pi$

- Let $\pi_i$ be the suffix of $\pi$ starting at $i \geq 0$
Formal Semantics of LTL (II)

The relation $\models$ is defined inductively as follows:

- $\pi \models p$ iff $p \in \text{Lab}(s_0)$
- $\pi \models \neg \psi$ iff not $\pi \models \psi$
- $\pi \models \psi_1 \lor \psi_2$ iff $\pi \models \psi_1$ or $\pi \models \psi_2$
- $\pi \models X\psi$ iff $\pi_1 \models \psi$
- $\pi \models \psi_1 \mathcal{U} \psi_2$ iff $\exists i \geq 0$, such that $\pi_i \models \psi_2$ and $\forall 0 \leq j < i$, we have that $\pi_j \models \psi_1$
Formal Semantics of LTL (III)

- Derived operators:
  
  - $\pi \models \psi_1 \land \psi_2$ iff $\pi \models \psi_1$ and $\pi \models \psi_2$
  
  - $\pi \models F\psi$ iff $\exists i \geq 0, \pi_i \models \psi$
  
  - $\pi \models G\psi$ iff $\forall i \geq 0, \pi_i \models \psi$
Additional operators: Weak Until (I)

- It is the Until in which the stop condition is not required to occur anymore.
- Thus, $\psi_1 W \psi_2$ is true if one between $\psi_1 U \psi_2$ and $G \psi_1$ holds.
- Formal semantics:
  - $\pi \models \psi_1 W \psi_2$ iff $\forall i \geq 1$, $\pi_i \models \psi_1$ or
    $\exists i \geq 0$, such that $\pi_i \models \psi_2$ and
    $\forall 0 \leq j < i$, we have that $\pi_j \models \psi_1$
- Also for $W$ it holds that $\psi_1 W \psi_2 = \psi_2 \lor (\psi_1 \land X (\psi_1 W \psi_2))$
Additional operators: Weak Until (II)

$p W q$

\[\begin{array}{c}
 s_0 \quad s_1 \quad s_2 \quad s_3 \\
p \quad p \quad p \quad \Box \\
 s_0 \quad s_1 \quad s_2 \quad s_3 \\
p \quad p \quad q \quad \Box \\
 s_0 \quad s_1 \quad s_2 \quad s_3 \\
p \quad p \quad p \quad p
\end{array}\]
Additional operators: Release (I)

- $\psi_1 \ R \ \psi_2$ :
  - $\psi_2$ is true until and including once $\psi_1$ becomes true, or
  - $\psi_2$ remains true forever

- Formal semantics:
  - $\pi \models \psi_1 \ R \ \psi_2$ iff $\forall \ i \geq 0$, $\pi_i \models \psi_2$ or $\exists \ i \geq 0$ such that $\pi_i \models \psi_1$ and $\forall \ 0 \leq j \leq i$, we have that $\pi_j \models \psi_2$

- The Release is the dual of the Until

- Some abbreviations: $\psi_1 \ R \ \psi_2 = \neg \neg \psi_1 \ U \ \neg \psi_2 = \psi_2 \land (\psi_1 \lor X(\psi_1 \ R \ \psi_2))$
Additional operators: Release (II)

$p R q$

\[
\begin{array}{cccc}
  s_0 & s_1 & s_2 & s_3 \\
  q & q & q & p \\
  s_0 & s_1 & s_2 & s_3 \\
  q & q & p,q & s_3 \\
  s_0 & s_1 & s_2 & s_3 \\
  q & q & q & q \\
\end{array}
\]
### Classical (Modal) Temporal operators

<table>
<thead>
<tr>
<th>Classical Symbol</th>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>○</td>
<td>X</td>
<td>Next</td>
</tr>
<tr>
<td>◇</td>
<td>F</td>
<td>Eventually (in the future)</td>
</tr>
<tr>
<td>□</td>
<td>G</td>
<td>Always (globally)</td>
</tr>
<tr>
<td>U</td>
<td>U</td>
<td>Strong until</td>
</tr>
<tr>
<td></td>
<td>W</td>
<td>Weak until</td>
</tr>
<tr>
<td></td>
<td>R</td>
<td>Release</td>
</tr>
</tbody>
</table>
Example of Specification: Ticket Machine

- “After any introduction of a new card, if tickets are released, the card will be ejected”

- In First-order logic:

\[ \forall t_0 \ [\text{Intro\_card}(t_0) \land (\exists t_1 > t_0 \ (\text{Tickets}(t_1) \land (\forall t_2, t_0 \leq t_2 \leq t_1 \Rightarrow \neg \text{Intro\_card}(t_2))))] \]
\[ \Rightarrow \exists t_3 > t_0 \ [\text{Eject\_card}(t_3) \land (\forall t_4, t_0 \leq t_4 \leq t_3 \Rightarrow \neg \text{Intro\_card}(t_4))] \]

- In LTL:

\[ \text{G} \ [\text{Intro\_card} \land \text{X}(\neg \text{Intro\_card} \lor \text{Tickets}) \Rightarrow \text{X}(\neg \text{Intro\_card} \lor \text{Eject\_card})] \]
LTL Model Checking

Given a Kripke structure $M = (AP, S, S_0, R, Lab)$ modelling the system and an LTL formula $\psi$ over $AP$ representing the specification.

The LTL model checking problem is to check whether

$$\pi \models \psi$$

for each path $\pi$ starting in $s_0 \in S_0$
LTL Satisfiability

Given a temporal logic formula $\psi$, is there a model satisfying $\psi$?

Examples:
- $\psi_1 = p \cup q$ is satisfiable
- $\psi_2 = (p \cup q) \land \neg q$ is not satisfiable