Topics in Verification

AZADEH FARZAN
FALL 2017
Model Checking
Option 1 for properties beyond reachability ...
One TS as a Spec for Another TS!

Given a TS M for the model and a TS S for the specification:
One TS as a Spec for Another TS!

Given a TS $M$ for the model and a TS $S$ for the specification:

Question: Is every behaviour of $M$ a behaviour of $S$?
One TS as a Spec for Another TS!

Given a TS $M$ for the model and a TS $S$ for the specification:

Question: Is every behaviour of $M$ a behaviour of $S$?

$L(M) \subseteq L(S)$
One TS as a Spec for Another TS!

Given a TS $M$ for the model and a TS $S$ for the specification:

Question: Is every behaviour of $M$ a behaviour of $S$?

$$L(M) \subseteq L(S)$$

Solvable in PSpace: linear in $M$ and exponential in $S$. 
Best choice: new logic!
Alternative: Temporal Logic

- Language for describing properties of infinite sequences.
- Extension of propositional logic.
- Uses temporal operators to describe sequencing properties.
Linear Temporal Temporal Logic
5.1.1 Syntax

This subsection describes the syntactic rules according to which formulae in LTL can be constructed. The basic ingredients of LTL-formulae are atomic propositions (state labels $a \in AP$), the Boolean connectors like conjunction $\land$, and negation $\neg$, and two basic temporal modalities $\Box$ (pronounced "next") and $U$ (pronounced "until"). The atomic proposition $a \in AP$ stands for the state label $a$ in a transition system. Typically, the atoms are assertions about the values of control variables (e.g., locations in program graphs) or the values of program variables such as "$x > 5$" or "$x \leq y$". The $\Box$-modality is a unary prefix operator and requires a single LTL formula as argument. Formula $\Box \varphi$ holds at the current moment, if $\varphi$ holds in the next "step". The $U$-modality is a binary infix operator and requires two LTL formulae as argument. Formula $\varphi_1 U \varphi_2$ holds at the current moment, if there is some future moment for which $\varphi_2$ holds and $\varphi_1$ holds at all moments until that future moment.

Definition 5.1. Syntax of LTL

LTL formulae over the set $AP$ of atomic propositions are formed according to the following grammar:

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \land \varphi_2 \mid \neg \varphi \mid \Box \varphi \mid \varphi_1 U \varphi_2$$

where $a \in AP$.

The Backus Naur form (BNF) is used in a somewhat liberal way. More concretely, nonterminals are identified with derived words (formulae) and indices in the rules. Moreover, brackets will be used, e.g. in $a \land (b U c)$, which are not shown in the grammar. Such simplified notations for grammars to determine the syntax of formulae of some logic (or terms of other calculi) are often called abstract syntax.
LTL Syntax

\[ \varphi ::= \text{true} \mid a \mid \varphi_1 \land \varphi_2 \mid \neg \varphi \mid \Box \varphi \mid \varphi_1 \mathbf{U} \varphi_2 \]

\( a \in AP \)
LTL Syntax

\[ \varphi ::= \text{true} \mid a \mid \varphi_1 \land \varphi_2 \mid \neg \varphi \mid \Box \varphi \mid \varphi_1 \mathbf{U} \varphi_2 \]

\[ a \in AP \]

\[ \Diamond \varphi \overset{\text{def}}{=} \text{true} \mathbf{U} \varphi \quad \quad \Box \varphi \overset{\text{def}}{=} \neg \Diamond \neg \varphi \]
LTL: Intuition
Before proceeding with the formal semantics of LTL, we present some examples.

Example 5.2. Properties for the Mutual Exclusion Problem

Consider the mutual exclusion problem for two concurrent processes $P_1$ and $P_2$, say. Process $P_i$ is modeled by three locations: (1) the noncritical section, (2) the waiting phase which is entered when the process intends to enter the critical section, and (3) the critical section. Let the propositions $\text{wait}_i$ and $\text{crit}_i$ denote that process $P_i$ is in its waiting phase and critical section, respectively.

The safety property stating that $P_1$ and $P_2$ never simultaneously have access to their critical sections can be described by the LTL-formula:

$$\Box (\neg \text{crit}_1 \lor \neg \text{crit}_2)$$

This formula expresses that always ($\Box$) at least one of the processes is not in its critical section ($\neg \text{crit}_i$).

The liveness requirement stating that each process $P_i$ is infinitely often in its critical section can be described by the LTL-formula:

$$\Diamond \Box \text{crit}_i$$
LTL Semantics

LTL is interpreted over paths.

These paths are (infinite) words labeled with subset of the atomic propositions (AP) that are true at each letter.
LTL Semantics

LTL is interpreted over paths.

These paths are (infinite) words labeled with subset of the atomic propositions (AP) that are true at each letter.

\[
\begin{align*}
\sigma & \models \text{true} \\
\sigma & \models a \quad \text{iff} \quad a \in A_0 \quad (\text{i.e.,} \ A_0 \models a) \\
\sigma & \models \varphi_1 \land \varphi_2 \quad \text{iff} \quad \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2 \\
\sigma & \models \neg \varphi \quad \text{iff} \quad \sigma \not\models \varphi \\
\sigma & \models \Diamond \varphi \quad \text{iff} \quad \sigma[1\ldots] = A_1A_2A_3\ldots \models \varphi \\
\sigma & \models \varphi_1 \mathbf{U} \varphi_2 \quad \text{iff} \quad \exists j \geq 0. \ \sigma[j\ldots] \models \varphi_2 \text{ and } \sigma[i\ldots] \models \varphi_1, \text{ for all } 0 \leq i < j
\end{align*}
\]
LTL Semantics

LTL is interpreted over paths.

These paths are (infinite) words labeled with subset of the atomic propositions (AP) that are true at each letter.

\[
\sigma \models \text{true} \\
\sigma \models a \quad \text{iff} \quad a \in A_0 \quad (\text{i.e., } A_0 \models a) \\
\sigma \models \varphi_1 \land \varphi_2 \quad \text{iff} \quad \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2 \\
\sigma \models \neg \varphi \quad \text{iff} \quad \sigma \not\models \varphi \\
\sigma \models \Box \varphi \quad \text{iff} \quad \sigma[1...] = A_1 A_2 A_3 \ldots \models \varphi \\
\sigma \models \varphi_1 \text{U} \varphi_2 \quad \text{iff} \quad \exists j \geq 0. \, \sigma[j...] \models \varphi_2 \text{ and } \sigma[i...] \models \varphi_1, \text{ for all } 0 \leq i < j
\]

LTL's \models is the smallest relation satisfying the above rules.
The semantics of the combinations of ∃ j extends as follows:

σ \models \lozenge \phi \iff

σ \models \Box \phi \iff

σ \models \Box \lozenge \phi \iff

σ \models \lozenge \Box \phi \iff
The semantics of the combinations of "next step".

As a subsequent step, we determine the semantics of LTL-formulae with respect to a

\[ \sigma \geq t r u e \]

and the semantics of

\[ \exists j. i<j \]

stands for

\[ \exists j. i \leq j \]

if

\[ A \]

iff

\[ \forall \]

iff

\[ \neg A \]

iff

\[ \forall j.0 \leq j \]

iff

\[ \exists j.0 \geq j \]

iff

\[ \neg \exists j.0 \geq j \]

iff

\[ \neg \forall j.0 \leq j \]

iff

\[ \exists j.0 < j \]

iff

\[ \forall j.0 > j \]

iff

\[ \neg \exists j.0 > j \]

iff

\[ \neg \forall j.0 < j \]

iff

\[ \exists j.0 \geq j \]

iff

\[ \forall j.0 \leq j \]

iff

\[ \neg \exists j.0 \leq j \]

iff

\[ \neg \forall j.0 > j \]
\[ \sigma \models \lozenge \varphi \iff \exists j \geq 0. \ \sigma[j\ldots] \models \varphi \]

\[ \sigma \models \Box \varphi \iff \forall j \geq 0. \ \sigma[j\ldots] \models \varphi \]

\[ \sigma \models \Box \lozenge \varphi \iff \exists j. \ \sigma[j\ldots] \models \varphi \]

\[ \sigma \models \lozenge \Box \varphi \iff \forall j. \ \sigma[j\ldots] \models \varphi \]
Examples

mutual exclusion:
Examples

mutual exclusion:

$$\Box(\neg \text{crit}_1 \lor \neg \text{crit}_2)$$
mutual exclusion: $\Box(\neg crit_1 \lor \neg crit_2)$

once red, the light cannot become green immediately:
Examples

mutual exclusion:

\[ \Box( \neg \text{crit}_1 \lor \neg \text{crit}_2 ) \]

once red, the light cannot become green immediately:

\[ \Box( \text{red} \rightarrow \neg \Diamond \text{green} ) \]
Examples

mutual exclusion:
\[ \Box (\neg \text{crit}_1 \lor \neg \text{crit}_2) \]

once red, the light cannot become green immediately:
\[ \Box (\text{red} \rightarrow \neg \Diamond \text{green}) \]

every request will eventually lead to a response:
Examples

mutual exclusion: \( □(\neg \text{crit}_1 \lor \neg \text{crit}_2) \)

once red, the light cannot become green immediately: \( □(\text{red} \rightarrow \neg \Diamond \text{green}) \)

every request will eventually lead to a response: \( □(\text{request} \rightarrow \Diamond \text{response}) \)
Examples

mutual exclusion:

\( \Box \left( \neg \text{crit}_1 \lor \neg \text{crit}_2 \right) \)

once red, the light cannot become green immediately:

\( \Box \left( \text{red} \rightarrow \neg \Diamond \text{green} \right) \)

every request will eventually lead to a response:

\( \Box \left( \text{request} \rightarrow \Diamond \text{response} \right) \)

once red, the light always becomes green eventually after being yellow for some time:
Examples

mutual exclusion: \( \square (\neg crit_1 \lor \neg crit_2) \)

once red, the light cannot become green immediately: \( \square (red \rightarrow \neg \Diamond green) \)

every request will eventually lead to a response: \( \square (request \rightarrow \Diamond response) \)

once red, the light always becomes green eventually after being yellow for some time:

\( \square (red \rightarrow \Diamond (red \lor (yellow \land \Diamond (yellow \lor green)))) \)
LTL Semantics

LTL semantics can be lifted from paths to states and transition systems.
LTL Semantics

LTL semantics can be lifted from paths to states and transition systems.

\[ s \models \phi \iff \forall \pi : \pi[0] = s \Rightarrow \pi \models \phi \]
LTL semantics can be lifted from paths to states and transition systems.

\[ s \models \phi \iff \forall \pi : \pi[0] = s \rightarrow \pi \models \phi \]

\[ TS \models \phi \iff \forall s \in I : s \models \phi \]
Examples

Consider the transition system $TS$ depicted in Figure 5.3 with the set of propositions $AP = \{a, b\}$. For example, we have that $TS \models □a$, since all states are labelled with $a$, and hence, all traces of $TS$ are words of the form $A_0 A_1 A_2 \ldots$ with $a \in A_i$ for all $i \geq 0$. Thus, $s_i \models □a$ for $i = 1, 2, 3$. Moreover:

- $s_1 \models □(a \land b)$ since $s_2 \models a \land b$ and $s_2$ is the only successor of $s_1$.
- $s_2 \not\models □(a \land b)$ and $s_3 \not\models □(a \land b)$ as $s_3 \in \text{Post}(s_2)$ and $s_3 \not\models a \land b$.

This yields $TS \not\models □(a \land b)$ as $s_3$ is an initial state for which $s_3 \not\models □(a \land b)$.

As another example:

- $TS \models □(\neg b \rightarrow □(a \land \neg b))$, since $s_3$ is the only $\neg b$ state, $s_3$ cannot be left anymore, and $a \land \neg b$ in $s_3$ is true. However, $TS \not\models b \mathcal{U} (a \land \neg b)$, since the initial path $(s_1 s_2 \omega)$ does not visit a state for which $a \land \neg b$ holds.

Remark 5.9. Semantics of Negation

For paths, it holds $\pi \models \varphi$ if and only if $\pi \not\models \neg \varphi$. This is due to the fact that $\text{Words}(\neg \varphi) = (\text{Words}(\varphi)) \setminus \omega$.
Examples

\[ s_1 \models \mathbb{G} (a \land b) \]
Examples

\[
\begin{align*}
{s_1} & \models \Box (a \land b) \\
{s_2} & \not\models \Box (a \land b)
\end{align*}
\]
Examples

\[ s_1 \models \bigcirc (a \land b) \]
\[ s_2 \not\models \bigcirc (a \land b) \]
\[ s_3 \not\models \bigcirc (a \land b) \]
Examples

$s_1 \models \Diamond (a \land b)$

$s_2 \not\models \Diamond (a \land b)$

$TS \not\models \Diamond (a \land b)$

$s_3 \not\models \Diamond (a \land b)$
Negation?

\[ \pi \models \phi \iff \pi \not\models \neg \phi \]
Negation?

\[ \pi \models \phi \iff \pi \not\models \neg \phi \]

This is for paths, what about transition systems?
Negation?

\[ \pi \models \phi \iff \pi \not\models \neg \phi \]

This is for paths, what about transition systems?
Negation?

\[ \pi \models \phi \iff \pi \not\models \neg \phi \]

This is for paths, what about transition systems?

![Transition System Diagram](image-url)
Definition. Two LTL formulas are equivalent iff:

\[ \forall \pi : \pi \models \phi_1 \iff \pi \models \phi_2 \]
**Equivalence of LTL Formulae**

<table>
<thead>
<tr>
<th>duality law</th>
<th>idempotency law</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$</td>
<td>$\bigcirc \varphi \equiv \bigcirc \varphi$</td>
</tr>
<tr>
<td>$\neg \Diamond \varphi \equiv \Box \neg \varphi$</td>
<td>$\Box \Box \varphi \equiv \Box \varphi$</td>
</tr>
<tr>
<td>$\neg \Box \varphi \equiv \Diamond \neg \varphi$</td>
<td>$\varphi U (\varphi U \psi) \equiv \varphi U \psi$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>absorption law</th>
<th>expansion law</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Diamond \Box \Diamond \varphi \equiv \Box \Diamond \varphi$</td>
<td>$\varphi U \psi \equiv \psi \lor (\varphi \land \bigcirc (\varphi U \psi))$</td>
</tr>
<tr>
<td>$\Box \Diamond \Box \varphi \equiv \Diamond \Box \varphi$</td>
<td>$\Diamond \psi \equiv \psi \lor \bigcirc \Diamond \psi$</td>
</tr>
<tr>
<td>$\Box \Diamond \Box \varphi \equiv \Diamond \Box \varphi$</td>
<td>$\Box \psi \equiv \psi \land \bigcirc \Box \psi$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>distributive law</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bigcirc (\varphi U \psi) \equiv (\bigcirc \varphi) U (\bigcirc \psi)$</td>
</tr>
<tr>
<td>$\Diamond (\varphi \lor \psi) \equiv \Diamond \varphi \lor \Diamond \psi$</td>
</tr>
<tr>
<td>$\Box (\varphi \land \psi) \equiv \Box \varphi \land \Box \psi$</td>
</tr>
</tbody>
</table>
Expansion Laws

<table>
<thead>
<tr>
<th>Formula</th>
<th>Equivalent</th>
<th>Simplified</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi U \psi$</td>
<td>$\psi \lor (\varphi \land \Diamond (\varphi U \psi))$</td>
<td></td>
</tr>
<tr>
<td>$\Diamond \psi$</td>
<td>$\psi \lor \Diamond \Diamond \psi$</td>
<td></td>
</tr>
<tr>
<td>$\Box \psi$</td>
<td>$\psi \land \Box \Box \psi$</td>
<td></td>
</tr>
</tbody>
</table>
Lemma. Until is the least solution to the expansion law.

Expansion Laws

\[\varphi \mathsf{U} \psi \equiv \psi \lor (\varphi \land \mathsf{O}(\varphi \mathsf{U} \psi))\]

\[\Diamond \psi \equiv \psi \lor \mathsf{O} \Diamond \psi\]

\[\Box \psi \equiv \psi \land \mathsf{O} \Box \psi\]
**Expansion Laws**

<table>
<thead>
<tr>
<th>Expansion Law</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \varphi U \psi )</td>
<td>( \psi \lor (\varphi \land \Diamond (\varphi U \psi)) )</td>
</tr>
<tr>
<td>( \Diamond \psi )</td>
<td>( \psi \lor \Diamond \Diamond \psi )</td>
</tr>
<tr>
<td>( \Box \psi )</td>
<td>( \psi \land \Diamond \Box \psi )</td>
</tr>
</tbody>
</table>

**Lemma.** Until is the least solution to the expansion law.

The following equation has many solutions:

\[
X = \psi \lor (\phi \land \Diamond X)
\]

Until is the smallest set that satisfies this equation.
Lemma. Until is the least solution to the expansion law.

The following equation has many solutions:

\[ X = \psi \lor (\phi \land \circ X) \]

Until is the smallest set that satisfies this equation.

Note that we are using the notions of sets (of paths) and formulas interchangeably, by referring to the set of paths that satisfy a given formula.