Probabilistic Model Checking

Alessandro Abate

Lecture 4, p2: Linear Temporal Logic
Modal logics

- Based on propositional logic
- Used to reason about objects with modalities (expressed via modal operators)
- In particular, modal operators qualify temporal expressions
- In this course we shall focus on two classes: LTL and CTL
  1. LTL: linear temporal logic
  2. CTL: computational tree logic
- Extension to CTL*
Syntax of LTL

- \( \varphi ::= true \mid a \mid \varphi \land \varphi \mid \neg \varphi \mid \Diamond \varphi \mid \varphi \mathbin{U} \varphi, \quad a \in AP \)

- alternative expression of more formulae

\[
\begin{align*}
\varphi_1 \lor \varphi_2 & = \neg (\neg \varphi_1 \land \neg \varphi_2) \\
\varphi_1 \Rightarrow \varphi_2 & = \neg \varphi_1 \lor \varphi_2
\end{align*}
\]

and of two temporal modalities

- \( \Diamond \varphi = \text{true} \mathbin{U} \varphi \)
- \( \Box \varphi = \neg \Diamond \neg \varphi \)
Alternative syntax in the literature

- you may encounter the following notations:

\[
\begin{align*}
X\varphi & : \bigcirc \varphi \\
F\varphi & : \Diamond \varphi \\
G\varphi & : \Box \varphi
\end{align*}
\]

(notation on left-hand side from [CGP99], on right-hand side from [BK08])

- past operators are possible (though not strictly necessary)
Semantics of LTL

\[ TS \models \varphi \text{ iff } \forall s \in I : s \models \varphi \]

(recall that \( I \) is the set of initial states), where

\[ s \models \varphi \text{ iff } \forall \pi \in Paths(s) : \pi \models \varphi \]
Semantics of LTL

$TS \models \varphi \iff \forall s \in I : s \models \varphi$

(recall that $I$ is the set of initial states), where

$s \models \varphi \iff \forall \pi \in Paths(s) : \pi \models \varphi$

and where (cf. LTL syntax)

\[
\begin{align*}
\pi &\models \text{true} \\
\pi &\models a \quad \text{iff} \quad a \in L(\pi[0]) \\
\pi &\models \varphi \land \psi \quad \text{iff} \quad \pi \models \varphi \land \pi \models \psi \\
\pi &\models \neg \varphi \quad \text{iff} \quad \pi \not\models \varphi \\
\pi &\models \Box \varphi \quad \text{iff} \quad \pi[1..] \models \varphi \\
\pi &\models \varphi \mathbf{U} \psi \quad \text{iff} \quad \exists i \geq 0 : \pi[i..] \models \psi \land \forall 0 \leq j < i : \pi[j..] \models \varphi
\end{align*}
\]
Alternative semantics of LTL

- let $\varphi$ be an LTL formula over $AP$, inducing the LT property

\[
Words(\varphi) = \{ \sigma \in (2^{AP})^\omega \mid \sigma \models \varphi \}
\]

where $(\sigma = A_0A_1 \ldots)$

\[
\sigma \models true
\]

\[
\sigma \models a \iff a \in A_0
\]

\ldots

- $TS \models \varphi$ iff $Traces(TS) \subseteq Words(\varphi)$
Alternative semantics of LTL

- Let \( \varphi \) be an LTL formula over \( AP \), inducing the LT property

\[
\text{Words}(\varphi) = \{ \sigma \in (2^{AP})^\omega \mid \sigma \models \varphi \}
\]

where \((\sigma = A_0A_1 \ldots)\)

\[
\sigma \models \text{true}
\]

\[
\sigma \models a \iff a \in A_0
\]

\[
\ldots
\]

- \( TS \models \varphi \) iff \( \text{Traces}(TS) \subseteq \text{Words}(\varphi) \)

- \( \varphi_1 \equiv \varphi_2 \) if \( \text{Words}(\varphi_1) = \text{Words}(\varphi_2) \)
LTL properties for the traffic light model

- how to express
  “the light is infinitely often red”
  by an LTL formula?
- □◊red
LTL properties for the traffic light model

- how to express
  
  “the light is infinitely often red”

  by an LTL formula?

  ▶ □◊ red

- how to express
  
  “once green, the light cannot become immediately red”

  by an LTL formula?

  ▶ □(green ⇒ ¬□ red)
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models \text{red} ? \)
Verification of LTL specs is over linear-time paths

▶ back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

▶ question: \( \pi \models \text{red} \)?

▶ answer: yes
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models \Diamond \Diamond \text{red} \)?
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models \Box \Box \text{red} \)?

- answer: no
Verification of LTL specs is over linear-time paths

⏩ back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

⏩ question: \( \pi \models \text{red} \mathbf{U} \text{green} ? \)
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

  $\pi : \begin{array}{ccccccccc}
  1 & - & 2 & - & 3 & - & 4 & - & 1 & - & 5 & \cdots
  \end{array}$

- question: $\pi \models \text{red U green}$?

- answer: yes, because $L(2) = \{\text{red, amber}\}$
Verification of LTL specs is over linear-time paths

back to the traffic light model, consider the following path:

$\pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots$

question: $\pi \models \Diamond \text{black}$?
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models \Diamond \text{black} \)?

- answer: yes
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models \Box \neg \text{red} \)?
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models \square \neg \text{red} \)?

- answer: no
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

  \[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models (\Diamond \text{black}) \cup (\bigcirc \text{red})? \)
Verification of LTL specs is over linear-time paths

- back to the traffic light model, consider the following path:

\[ \pi : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \rightarrow 5 \rightarrow \ldots \]

- question: \( \pi \models (\Diamond \text{black}) \cup (\Box \text{red})? \)

- answer: yes
Expansion laws

- describe temporal modalities recursively

1. formula $\varphi \mathsf{U} \psi$ is a solution of $k = \psi \lor (\varphi \land \Box k)$
Expansion laws

- describe temporal modalities recursively

1. formula \( \varphi \mathbf{U} \psi \) is a solution of \( k = \psi \lor (\varphi \land \Box k) \)

2. similarly,
   \[ \Diamond \psi = \text{true} \mathbf{U} \psi = \psi \lor (\text{true} \land \Box (\text{true} \mathbf{U} \psi)) = \psi \lor \Box \Diamond \psi \]
Expansion laws

- describe temporal modalities recursively

1. formula $\varphi \mathcal{U} \psi$ is a solution of $k = \psi \lor (\varphi \land \mathcal{O}k)$

2. similarly,
   
   $\Diamond \psi = \text{true} \mathcal{U} \psi = \psi \lor (\text{true} \land \mathcal{O}(\text{true} \mathcal{U} \psi)) = \psi \lor \mathcal{O}\Diamond \psi$

3. also $\Box \psi = \neg \Diamond \neg \psi = \psi \land \mathcal{O}\Box \psi$
Weak-Until and PNF

- weak-until is dual of until:
  \[ \varphi \ W \psi = (\varphi \ U \psi) \lor \Box \varphi \]

- it holds that
  \[ \neg(\varphi \ U \psi) = (\varphi \land \neg\psi) \ W (\neg\varphi \land \neg\psi) \]

**Definition**

Weak-Until Positive Normal Form for LTL: for \( a \in AP \)

\[ \varphi ::= \text{true} \mid \text{false} \mid a \mid \neg a \mid \varphi \land \varphi \mid \varphi \lor \varphi \mid \Diamond \varphi \mid \varphi \ U \varphi \mid \varphi \ W \varphi \]

- each LTL formula admits an equivalent in w-u PNF form
Classes of LTL specifications

question: what class of LTL formulas capture invariants?
Classes of LTL specifications

- question: what class of LTL formulas capture *invariants*?

- answer: \( \square \varphi \), where \( \varphi ::= \text{true} \mid a \mid \varphi \land \varphi \mid \neg \varphi \)
Classes of LTL specifications

- question: what class of LTL formulas capture *invariants*?

- answer: $\square \varphi$, where $\varphi ::= \text{true} \mid a \mid \varphi \land \varphi \mid \neg \varphi$

- example: $\square \neg \text{red}$
Classes of LTL specifications

- question: how is the class of safety properties characterized?
Classes of LTL specifications

- question: how is the class of safety properties characterized?

- answer: “nothing bad ever happens”
Classes of LTL specifications

- question: how is the class of safety properties characterized?
- answer: “nothing bad ever happens”
- example: “every red light is immediately preceded by amber”
- question: how can we express this property in LTL?
Classes of LTL specifications

- question: how is the class of safety properties characterized?
- answer: “nothing bad ever happens”
- example: “every red light is immediately preceded by amber”
- question: how can we express this property in LTL?
- answer: $\neg red \land \Box(\Diamond red \Rightarrow amber)$
Classes of LTL specifications

- question: how is the class of *liveness properties* characterized?
Classes of LTL specifications

- question: how is the class of *liveness properties* characterized?

- answer: “something good eventually happens”
Classes of LTL specifications

▷ question: how is the class of *liveness properties* characterized?

▷ answer: “something good eventually happens”

▷ example: “the light is infinitely often red”

▷ question: how can we express this property in LTL?
Classes of LTL specifications

▸ question: how is the class of *liveness properties* characterized?

▸ answer: “something good eventually happens”

▸ example: “the light is infinitely often red”

▸ question: how can we express this property in LTL?

▸ answer: □◊red
Liveness: an example

- consider traffic lights model

Diagram:

- question: is $\psi := \Box (black \Rightarrow \Diamond red)$ a liveness property?
Liveness: an example

- consider traffic lights model

question: is $\psi := \Box (black \Rightarrow \Diamond red)$ a liveness property?

answer: yes

and in fact $\mathcal{T}S \models \psi$
Fairness properties in LTL

- **unconditional fairness**: “every transition is infinitely often taken”
  \[\square\Diamond\psi\]

- **strong fairness**: “if a transition is infinitely often enabled, then it is infinitely often taken”
  \[\square\Diamond\phi \Rightarrow \square\Diamond\psi\]

- **weak fairness**: “if a transition is continuously enabled from a certain point in time, then it is infinitely often taken”
  \[\Diamond\square\phi \Rightarrow \square\Diamond\psi\]
Fairness properties as LTL constraints

- consider LTL constraint \textit{fair};
  \[ \text{FairPaths}(s) = \{ \pi \in \text{Paths}(s) \mid \pi \models \text{fair} \} \]
  \[ \rightarrow \text{FairPaths}(TS) \]
Fairness properties as LTL constraints

- consider LTL constraint $fair$;
  $$\text{FairPaths}(s) = \{ \pi \in \text{Paths}(s) \mid \pi \models fair \}$$
  $$\text{FairPaths}(TS)$$

- consider LTL specification $\varphi$;
  $$s \models_{\text{fair}} \varphi \iff \forall \pi \in \text{FairPaths}(s), \pi \models \varphi$$
  $$TS \models_{\text{fair}} \varphi$$
Fairness properties as LTL constraints

► consider LTL constraint \(\text{fair}\);
\[
\text{FairPaths}(s) = \{ \pi \in \text{Paths}(s) \mid \pi \models \text{fair} \}
\]
\[\rightarrow \text{FairPaths}(TS)\]

► consider LTL specification \(\varphi\);
\[
s \models_{\text{fair}} \varphi \leftrightarrow \forall \pi \in \text{FairPaths}(s), \pi \models \varphi
\]
\[\rightarrow TS \models_{\text{fair}} \varphi\]

► fairness constraints are easily embedded with LTL verification:
\[
TS \models_{\text{fair}} \varphi \Leftrightarrow TS \models (\text{fair} \Rightarrow \varphi)
\]
Fairness: an example

- consider the traffic lights model

- question: “is the traffic light infinitely often orange (amber and red)” under the strong fairness condition (if a transition is infinitely often enabled then it is infinitely often taken)?
Fairness: an example

- consider the traffic lights model

question: “is the traffic light infinitely often orange (amber and red)” under the strong fairness condition (if a transition is infinitely often enabled then it is infinitely often taken)?

answer: no
Fairness: an example

- consider the traffic lights model

![](image)

- question: “is the traffic light infinitely often orange (amber and red)” under the strong fairness condition (if a transition is infinitely often enabled then it is infinitely often taken)?

- answer: no

- this fairness condition can be expressed in LTL as: 
  \((\Box \Diamond \text{red}) \Rightarrow \Box \Diamond (\text{red} \land \Diamond \text{orange})\)
Fairness: a second example

- consider the traffic lights model

[Diagram]

- question: “is the traffic light infinitely often orange” under the weak fairness condition (if a transition is continuously enabled from a certain point in time then it is infinitely often taken)?
Fairness: a second example

- consider the traffic lights model

question: “is the traffic light infinitely often orange” under the weak fairness condition (if a transition is continuously enabled from a certain point in time then it is infinitely often taken)?

answer: yes
Fairness: a second example

▶ consider the traffic lights model

question: “is the traffic light infinitely often orange” under the weak fairness condition (if a transition is continuously enabled from a certain point in time then it is infinitely often taken)?

▶ answer: yes

▶ this fairness condition can be expressed in LTL as:

$(\mathcal{G} \mathcal{F} \text{red}) \Rightarrow \mathcal{F} \mathcal{G} (\text{red} \land \Diamond \text{orange})$
Expressiveness of LTL

- question: are there temporal properties that we cannot express in LTL?
- answer: yes
- example: “always a state satisfying $a$ can be reached”
- consider expression

\[
\forall \pi \in Paths(TS) : \forall m \geq 0 : \exists \pi' \in Paths(\pi[m]) : \exists n \geq 0 : \pi'[n] \models a
\]

- there does not exists an LTL formula $\varphi$ so that $TS \models \varphi$
LTL Quiz

- (semantics of negation)
- argue why \((TS \not\models \varphi) \not\equiv (TS \models \neg \varphi)\)
LTL Quiz

▸ (semantics of negation)
▸ argue why \((TS \not\models \varphi) \not\equiv (TS \models \neg \varphi)\)

▸ and why instead \(\models \neg \varphi \Rightarrow TS \not\models \varphi\)
Today’s reading material

- Section 5.1 of