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

- $\varphi ::= \text{true} \mid a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \,\mathsf{U}\, \varphi, \quad a \in AP$
- alternative expression of more formulae

$$\begin{array}{rcl} \varphi_1 \vee \varphi_2 & = & \neg(\neg\varphi_1 \wedge \neg\varphi_2) \\ \varphi_1 \Rightarrow \varphi_2 & = & \neg\varphi_1 \vee \varphi_2 \end{array}$$

and of two temporal modalities

$$\begin{array}{rcl} \Diamond\varphi & = & \text{true} \,\mathsf{U}\, \varphi \\ \Box\varphi & = & \neg\Diamond\neg\varphi \end{array}$$

Alternative syntax in the literature

- you may encounter the following notations:

$$\begin{array}{lcl} \mathsf{X}\varphi & : & \bigcirc\varphi \\ \mathsf{F}\varphi & : & \Diamond\varphi \\ \mathsf{G}\varphi & : & \Box\varphi \end{array}$$

(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

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

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

$$s \models \varphi \text{ iff } \forall \pi \in \mathit{Paths}(s) : \pi \models \varphi$$

and where (cf. LTL syntax)

$$\begin{array}{rcl}
\pi \models \text{true} & & \\
\pi \models a & \text{iff} & a \in L(\pi[0]) \\
\pi \models \varphi \wedge \psi & \text{iff} & \pi \models \varphi \wedge \pi \models \psi \\
\pi \models \neg\varphi & \text{iff} & \pi \not\models \varphi \\
\pi \models \bigcirc\varphi & \text{iff} & \pi[1..] \models \varphi \\
\pi \models \varphi \,\mathsf{U}\, \psi & \text{iff} & \exists i \geq 0 : \pi[i..] \models \psi \wedge \forall 0 \leq j < i : \pi[j..] \models \varphi
\end{array}$$

Alternative semantics of LTL

- let φ be an LTL formula over AP, inducing the LT property

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

where ($\sigma = A_0A_1\ldots$)

$$\begin{aligned}
\sigma &\models \text{ true} \\
\sigma &\models a \Leftrightarrow a \in A_0 \\
&\ldots
\end{aligned}$$

- $TS \models \varphi$ iff $Traces(TS) \subseteq Words(\varphi)$

Alternative semantics of LTL

- let φ be an LTL formula over AP, inducing the LT property

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

where ($\sigma = A_0 A_1 \ldots$)

$$\begin{aligned} \sigma &\models \text{true} \\ \sigma &\models a \Leftrightarrow a \in A_0 \\ &\ldots \end{aligned}$$

- $TS \models \varphi$ iff $Traces(TS) \subseteq Words(\varphi)$
- $\varphi_1 \equiv \varphi_2$ if $Words(\varphi_1) = Words(\varphi_2)$

LTL properties for the traffic light model

- how to express
  "the light is infinitely often red"
  by an LTL formula?
- $\Box\Diamond$red

LTL properties for the traffic light model

- how to express

  "the light is infinitely often red"

  by an LTL formula?
- $\Box\Diamond \text{red}$
- how to express

  "once green, the light cannot become immediately red"

  by an LTL formula?
- $\Box(\text{green} \Rightarrow \neg\bigcirc \text{red})$

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

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

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- question: $\pi \models$ red?
- answer: yes

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

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

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- question: $\pi \models \bigcirc\bigcirc$red?
- answer: no

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- question: $\pi \models$ red U green?

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

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

- answer: yes, because $L(2) = \{\mathsf{red}, \mathsf{amber}\}$

Verification of LTL specs is over linear-time paths

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

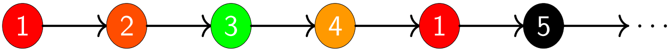
$$\pi : \quad 1 \to 2 \to 3 \to 4 \to 1 \to 5 \to \cdots$$

- 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:

$\pi :$



- question: $\pi \models \Diamond$black?
- answer: yes

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- 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:

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- question: $\pi \models \Box\neg\text{red}$?
- answer: no

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- question: $\pi \models (\Diamond \text{black}) \; \mathsf{U} \; (\bigcirc \text{red})$?

Verification of LTL specs is over linear-time paths

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

$$\pi : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 5 \longrightarrow \cdots$$

- question: $\pi \models (\Diamond \mathsf{black})\ \mathsf{U}\ (\bigcirc \mathsf{red})$?

- answer: yes

Expansion laws

- describe temporal modalities recursively

1. formula $\varphi \, \mathsf{U} \, \psi$ is a solution of $k = \psi \vee (\varphi \wedge \bigcirc k)$

Expansion laws

- describe temporal modalities recursively

1. formula $\varphi \,\mathsf{U}\, \psi$ is a solution of $k = \psi \vee (\varphi \wedge \bigcirc k)$

2. similarly,
   $\Diamond\psi = \mathsf{true}\,\mathsf{U}\,\psi = \psi \vee (\mathsf{true} \wedge \bigcirc(\mathsf{true}\,\mathsf{U}\,\psi)) = \psi \vee \bigcirc\Diamond\psi$

Expansion laws

- describe temporal modalities recursively

1. formula $\varphi \, \mathsf{U} \, \psi$ is a solution of $k = \psi \vee (\varphi \wedge \bigcirc k)$
2. similarly,
   $\Diamond\psi = \mathsf{true} \, \mathsf{U} \, \psi = \psi \vee (\mathsf{true} \wedge \bigcirc(\mathsf{true} \, \mathsf{U} \, \psi)) = \psi \vee \bigcirc\Diamond\psi$
3. also $\Box\psi = \neg\Diamond\neg\psi = \psi \wedge \bigcirc\Box\psi$

Weak-Until and PNF

- weak-until is dual of until:

$$\varphi \mathsf{W} \psi = (\varphi \mathsf{U} \psi) \vee \Box\varphi$$

- it holds that

$$\neg(\varphi \mathsf{U} \psi) = (\varphi \wedge \neg\psi) \mathsf{W} (\neg\varphi \wedge \neg\psi)$$

Definition

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

$$\varphi ::= \mathsf{true} \mid \mathsf{false} \mid a \mid \neg a \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \bigcirc\varphi \mid \varphi \mathsf{U} \varphi \mid \varphi \mathsf{W} \varphi$$

- 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: $\Box\varphi$, where $\varphi ::= \mathsf{true} \mid a \mid \varphi \land \varphi \mid \neg\varphi$

Classes of LTL specifications

- question: what class of LTL formulas capture *invariants*?
- answer: $\Box\varphi$, where $\varphi ::= \mathsf{true} \mid a \mid \varphi \wedge \varphi \mid \neg\varphi$
- example: $\Box\neg\mathsf{red}$

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: $\neg \mathsf{red} \wedge \Box(\bigcirc \mathsf{red} \Rightarrow \mathsf{amber})$

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

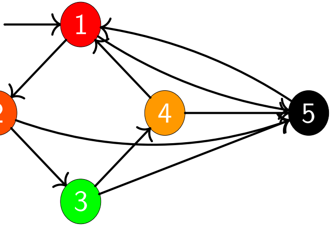
- question: how is the class of *liveness properties* characterized?
- answer: "something good eventually happens"
- example: "the light is infinitely often red"
- question: how can we express this property in LTL?

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: $\Box\Diamond \mathit{red}$

Liveness: an example

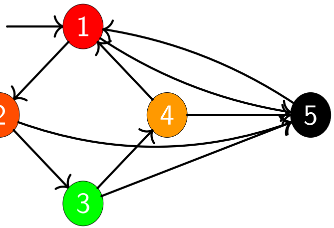
- consider traffic lights model



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

Liveness: an example

- consider traffic lights model



- question: is $\psi := \Box(\mathit{black} \Rightarrow \Diamond \mathit{red})$ a liveness property?
- answer: yes
- and in fact $\mathit{TS} \models \psi$

Fairness properties in LTL

- *unconditional fairness:* "every transition is infinitely often taken"

$$\Box\Diamond\Psi$$

- *strong fairness:* "if a transition is infinitely often enabled, then it is infinitely often taken"

$$\Box\Diamond\Phi \Rightarrow \Box\Diamond\Psi$$

- *weak fairness:* "if a transition is continuously enabled from a certain point in time, then it is infinitely often taken"

$$\Diamond\Box\Phi \Rightarrow \Box\Diamond\Psi$$

Fairness properties as LTL constraints

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

$\rightarrow$ $\mathit{FairPaths}(\mathit{TS})$

Fairness properties as LTL constraints

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

$\rightarrow$ $FairPaths(TS)$

- consider LTL specification φ;
  $s \models_{fair} \varphi \Leftrightarrow \forall \pi \in FairPaths(s), \pi \models \varphi$

$\rightarrow$ $TS \models_{fair} \varphi$

Fairness properties as LTL constraints

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

$\rightarrow$ $FairPaths(TS)$

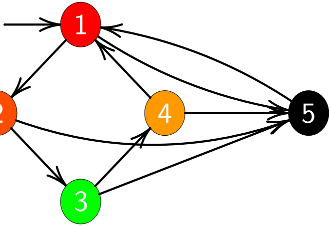
- consider LTL specification φ;
  $s \models_{fair} \varphi \Leftrightarrow \forall \pi \in FairPaths(s), \pi \models \varphi$

$\rightarrow$ $TS \models_{fair} \varphi$

- fairness constraints are easily embedded with LTL verification:
  $TS \models_{fair} \varphi \Leftrightarrow TS \models (fair \Rightarrow \varphi)$

Fairness: an example

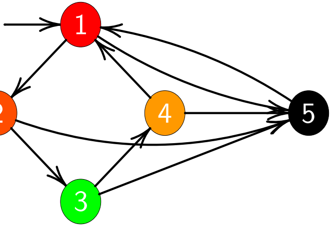
- consider the traffic lights model



- 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

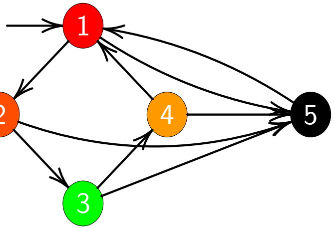


- question: "is the traffic light infinitely often orange (amber and red)" under the strong fairness condition (if a transition is infinitely often enabled then it is infinitely often taken)?

- answer: no

Fairness: an example

- consider the traffic lights model



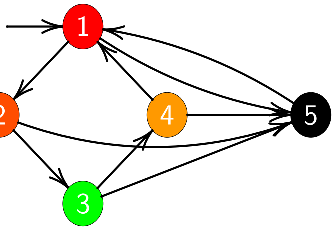
- question: "is the traffic light infinitely often orange (amber and red)" under the strong fairness condition (if a transition is infinitely often enabled then it is infinitely often taken)?

- answer: no

- this fairness condition can be expressed in LTL as:
  $(\Box\Diamond \text{red}) \Rightarrow \Box\Diamond(\text{red} \wedge \bigcirc \text{orange})$

Fairness: a second example

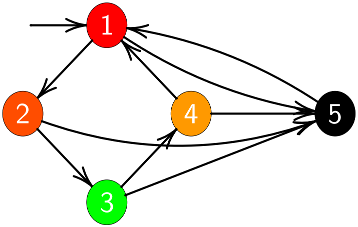
- consider the traffic lights model



- 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)?

Fairness: a second example

- consider the traffic lights model

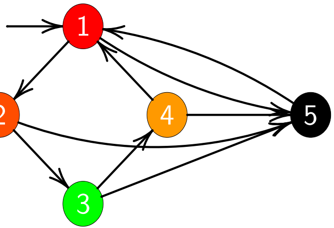


- question: "is the traffic light infinitely often orange" under the weak fairness condition (if a transition is continuously enabled from a certain point in time then it is infinitely often taken)?

- 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: $(\Diamond\Box \text{red}) \Rightarrow \Box\Diamond(\text{red} \wedge \bigcirc \text{orange})$

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

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

- there does not exists an LTL formula φ so that $\mathit{TS} \models \varphi$

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 $TS \models \neg\varphi \Rightarrow TS \not\models \varphi$

Today's reading material

- Section 5.1 of
  - Christel Baier and Joost-Pieter Katoen, *Principles of Model Checking*. The MIT Press. Cambridge, MA, USA. 2008.