Concurrent Object Oriented Languages

Linear Temporal Logic

wiki.eecs.yorku.ca/course/6490A

Linear temporal logic (LTL) was proposed by Amir Pnueli to verify computer systems.

Amir Pnueli (1941–2009)

- Recipient of the Turing Award (1996)
- Recipient of the Israel prize (2000)
- Foreign Associate of the U.S. National Academy of Engineering (1999)
- Fellow of the Association for Computing Machinery (2007)

Source: David Monniaux

Syntax of LTL

$$\varphi ::= \mathsf{true} \mid a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \,\mathsf{U}\, \varphi$$

Syntax for LTL

$$\varphi ::= \text{true} \mid a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \, \mathbf{U} \, \varphi$$

Question

What is the syntactic sugar for $\varphi_1 \vee \varphi_2$?

Syntax for LTL

$$\varphi ::= \text{true} \mid a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \, \mathsf{U} \, \varphi$$

Question

What is the syntactic sugar for $\varphi_1 \vee \varphi_2$?

Answer

$\neg(\neg\varphi_1 \wedge \neg\varphi_2)$.

Syntactic sugar

$$
\begin{aligned}
\varphi_1 \vee \varphi_2 &= \neg(\neg\varphi_1 \wedge \neg\varphi_2) \\
\varphi_1 \Rightarrow \varphi_2 &= \neg\varphi_1 \vee \varphi_2 \\
\Diamond\varphi &= \text{true}\ \mathsf{U}\ \varphi \\
\Box\varphi &= \neg\Diamond\neg\varphi
\end{aligned}
$$

Alternative syntax

$$\begin{aligned} \mathrm{X}\varphi &: \bigcirc\varphi \\ \mathrm{F}\varphi &: \Diamond\varphi \\ \mathrm{G}\varphi &: \Box\varphi \end{aligned}$$

Express properties

Question

How do you express in LTL that “the light is infinitely often red”?

Express properties

Question

How do you express in LTL that “the light is infinitely often red”?

Answer

$\Box\Diamond red$

Question

How do you express in LTL that “once green, the light cannot become red immediately”?

Express properties

Question

How do you express in LTL that “once green, the light cannot become red immediately”?

Answer

$\Box(\text{green} \Rightarrow \neg \bigcirc \text{red})$

Semantics of LTL

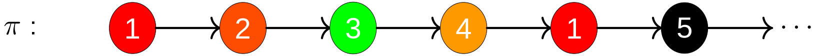
$$TS \models \varphi \text{ iff } \forall s \in I : s \models \varphi$$

where

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

where

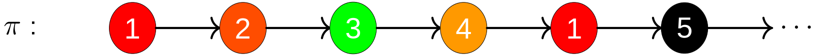
$$\begin{array}{rll}
\pi \models \text{true} & & \\
\pi \models a & \text{iff} & a \in L(\pi[0]) \\
\pi \models \varphi \wedge \psi & \text{iff} & \pi \models \varphi \wedge \pi \models \psi \\
\pi \models \neg\varphi & \text{iff} & \pi \not\models \varphi \\
\pi \models \bigcirc\varphi & \text{iff}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



Question

$\pi \models$ red?

Semantics of LTL



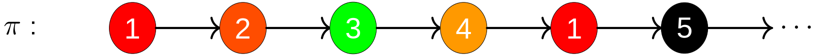
Question

$\pi \models$ red?

Answer

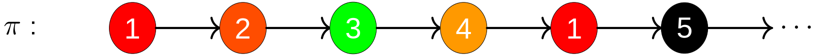
Yes.

Semantics of LTL



Question

$\pi \models \bigcirc\bigcirc \text{red}$?



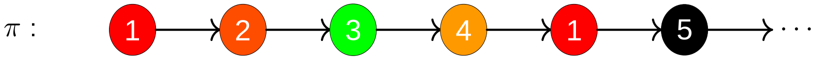
Question

$\pi \models \bigcirc\bigcirc \text{red}$?

Answer

No.

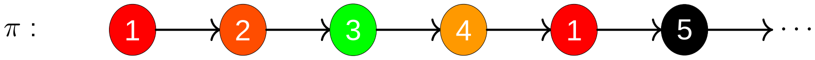
Semantics of LTL



Question

$\pi \models$ red U green?

Semantics of LTL

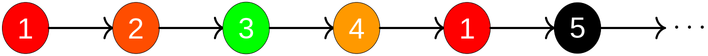


Question

$\pi \models$ red U green?

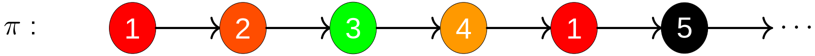
Answer

Yes, because $L(2) = \{$red, amber$\}$.

π : 

Question

$\pi \models \Diamond$black?



Question

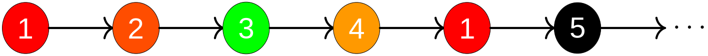
$\pi \models \Diamond$black?

Answer

Yes.

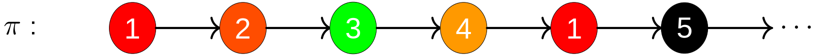
Semantics of LTL

π :



Question

$\pi \models \Box \neg$red?



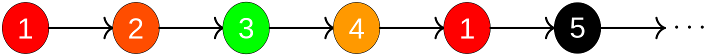
Question

$\pi \models \Box\neg$red?

Answer

No.

π :

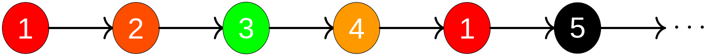


Question

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

Semantics of LTL

π :



Question

$\pi \models$ ($\Diamond$black) U $\bigcirc$red)?

Answer

Yes.

Invariants

Definition

The class of LTL formulas $\Box\varphi$, where $\varphi ::= \text{true} \mid a \mid \varphi \wedge \varphi \mid \neg\varphi$ capture *invariants*.

Example

$\Box\neg$red.

Safety properties

The class of LTL formulas that capture that "Nothing bad ever happens" are called *safety properties*.

Example

"A red light is immediately preceded by amber"

Question

How can we express this property in LTL?

Safety properties

The class of LTL formulas that capture that “Nothing bad ever happens” are called *safety properties*.

Example

“A red light is immediately preceded by amber”

Question

How can we express this property in LTL?

Answer

$\Box(\bigcirc \text{red} \Rightarrow \text{amber})$.

Liveness properties

The class of LTL formulas that capture that “Something good eventually happens” are called *liveness properties*.

Example

“the light is infinitely often red”?

Question

How can we express this property in LTL?

Liveness properties

The class of LTL formulas that capture that “Something good eventually happens” are called *liveness properties*.

Example

“the light is infinitely often red”?

Question

How can we express this property in LTL?

Answer

$\Box\Diamond red$.

Question

Are there properties we cannot express in LTL?

Question

Are there properties we cannot express in LTL?

Answer

Yes.

Expressiveness of LTL

Question

Are there properties we cannot express in LTL?

Answer

Yes.

Example

“Always a state satisfying *a* can be reached”

Definition

The predicate $AR_a(TS)$ is defined by

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

Theorem

There does not exists an LTL formula φ with $TS \models \varphi$ iff $AR_a(TS)$.