Logics

EECS 4315

www.eecs.yorku.ca/course/4315/

Semantics of LTL

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

where

$$s \models f \text{ iff } \forall p \in Paths(s) : p \models f$$

where

$$\begin{array}{rcl}
p \models a & \text{iff} & a \in L(p[0]) \\
p \models f_1 \wedge f_2 & \text{iff} & p \models f_1 \wedge p \models f_2 \\
p \models \neg f & \text{iff} & p \not\models f \\
p \models \bigcirc f & \text{iff} & p[1..] \models f \\
p \models f_1 \text{ U } f_2 & \text{iff} & \exists i \geq 0 : p[i..] \models f_2 \wedge \forall 0 \leq j < i : p[j..] \models f_1
\end{array}$$

Equivalence

Definition

The LTL formulas f and g are equivalent, denoted $f \equiv g$, if for all transition systems TS,

$$TS \models f \text{ iff } TS \models g.$$

Equivalence

Definition

The LTL formulas f and g are equivalent, denoted $f \equiv g$, if for all transition systems TS,

$$TS \models f \text{ iff } TS \models g.$$

Exercise

Are the following formulas equivalent? Either provide a proof or a counter example.

(a) $\Diamond(f \wedge g) \equiv \Diamond f \wedge \Diamond g$?

(b) $\Diamond \bigcirc f \equiv \bigcirc \Diamond f$?

Invariants

Definition

The class of LTL formulas that capture *invariants* is defined by $\Box g$, where

$$g ::= a \mid g \wedge g \mid \neg g.$$

Invariants

Definition

The class of LTL formulas that capture *invariants* is defined by $\Box g$, where

$$g ::= a \mid g \wedge g \mid \neg g.$$

Example

$\Box \neg \text{red}$.

Safety properties

Safety properties are characterized by “nothing bad ever happens.” For example, “a red light is immediately preceded by orange” is a safety property.

Safety properties

Safety properties are characterized by “nothing bad ever happens.” For example, “a red light is immediately preceded by orange” is a safety property.

Question

How can we express this property in LTL?

Safety properties

Safety properties are characterized by “nothing bad ever happens.” For example, “a red light is immediately preceded by orange” is a safety property.

Question

How can we express this property in LTL?

Answer

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

Liveness properties

Liveness properties are characterized by “something good eventually happens.” For example, “the light is infinitely often red” is a liveness property.

Liveness properties

Liveness properties are characterized by “something good eventually happens.” For example, “the light is infinitely often red” is a liveness property.

Question

How can we express this property in LTL?

Liveness properties

Liveness properties are characterized by “something good eventually happens.” For example, “the light is infinitely often red” is a liveness property.

Question

How can we express this property in LTL?

Answer

$\Box\Diamond$red.

Question

Are there properties we cannot express in LTL?

Expressiveness of LTL

Question

Are there properties we cannot express in LTL?

Answer

Yes, for example, "Always a state satisfying *a* can be reached"

Expressiveness of LTL

Theorem

There does not exists an LTL formula φ *with* $TS \models \varphi$ *iff*

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

How to Modify the Logic?

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

How to Modify the Logic?

$$\forall p \in \mathit{Paths}(\mathit{TS}) : \forall m \geq 0 : \overbrace{\exists p' \in \mathit{Paths}(p[m]) : \underbrace{\exists n \geq 0 : p'[n] \models a}_{\Diamond a}}^{\exists \Diamond a}$$

How to Modify the Logic?

$$\forall p \in \mathit{Paths}(TS) : \underbrace{\forall m \geq 0 : \overbrace{\exists p' \in \mathit{Paths}(p[m]) : \underbrace{\exists n \geq 0 : p'[n] \models a}_{\Diamond a}}^{\exists \Diamond a}}_{\Box \exists \Diamond a}$$

How to Modify the Logic?

$$\overbrace{\forall p \in \mathit{Paths}(\mathit{TS}) : \underbrace{\forall m \geq 0 : \overbrace{\exists p' \in \mathit{Paths}(p[m]) : \underbrace{\exists n \geq 0 : p'[n] \models a}_{\Diamond a}}^{\exists \Diamond a}}_{\Box \exists \Diamond a}}^{\forall \Box \exists \Diamond a}$$

How to Modify the Logic?

$$\overbrace{\exists p' \in \mathit{Paths}(p[m]) : \underbrace{\exists n \geq 0 : p'[n] \models a}_{\Diamond a}}^{\exists \Diamond a}$$

Recall that $p \models \Diamond a$ expresses that path p satisfies formula $\Diamond a$.

Question

$? \models \exists \Diamond a$.

How to Modify the Logic?

$$\overbrace{\exists p' \in Paths(p[m]) : \underbrace{\exists n \geq 0 : p'[n] \models a}_{\Diamond a}}^{\exists \Diamond a}$$

Recall that $p \models \Diamond a$ expresses that path p satisfies formula $\Diamond a$.

Question

$? \models \exists \Diamond a$.

Answer

There exists a path p starting in state s such that $p \models \Diamond a$, hence, $s \models \exists \Diamond a$.

How to Modify the Logic?

$$\overbrace{\exists p' \in \mathit{Paths}(p[m]) : \underbrace{\exists n \geq 0 : p'[n] \models a}_{\Diamond a}}^{\exists \Diamond a}$$

Recall that $p \models \Diamond a$ expresses that path p satisfies formula $\Diamond a$.

Question

$? \models \exists \Diamond a$.

Answer

There exists a path p starting in state s such that $p \models \Diamond a$, hence, $s \models \exists \Diamond a$.

Consequence

We should distinguish between *path formulas* and *state formulas*.

Syntax

The *state formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists g \mid \forall g$$

The *path formulas* are defined by

$$g ::= \bigcirc f \mid f \,\mathrm{U}\, f$$

Computation tree logic (CTL)

Edmund M. Clarke and E. Allen Emerson. Design and synthesis of synchronization skeletons using branching time temporal logic. In, Dexter Kozen, editor, *Proceedings of Workshop on Logic of Programs*, volume 131 of *Lecture Notes in Computer Science*, pages 52–71. Yorktown Heights, NY, USA, May 1981. Springer-Verlag.

Jean-Pierre Queille and Joseph Sifakis. Specification and verification of concurrent systems in CESAR. In, Mariangiola Dezani-Ciancaglini and Ugo Montanari, editors, *Proceedings of the 5th International Symposium on Programming*, volume 137 of *Lecture Notes in Computer Science*, pages 337–351. Torino, Italy, April 1982. Springer-Verlag.

Syntax

The *state formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists (f \; \mathsf{U} \; f) \mid \forall \bigcirc f \mid \forall (f \; \mathsf{U} \; f)$$

Computation Tree Logic

The *state formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists g \mid \forall g$$

The *path formulas* are defined by

$$g ::= \bigcirc f \mid f \, \mathrm{U} \, f$$

Syntactic sugar

$$\begin{array}{rcl}
\exists\Diamond f & = & \exists(\text{true U } f) \\
\forall\Diamond f & = & \forall(\text{true U } f) \\
\exists\Box f & = & \neg\forall(\text{true U } \neg f) \\
\forall\Box f & = & \neg\exists(\text{true U } \neg f)
\end{array}$$

Example

Question

How to express “Each red light is preceded by a green light” in CTL?

Example

Question

How to express "Each red light is preceded by a green light" in CTL?

Answer

$\neg red \wedge \forall \Box (green \vee \forall \bigcirc \neg red)$