Linear Temporal Logic

EECS 4315

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

Linear temporal logic

Definition

LTL is defined by the grammar

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

where a is an atomic proposition.

An atomic proposition represents a basic property (such as the value of a particular variable being even or a particular method being invoked).

Semantics of LTL

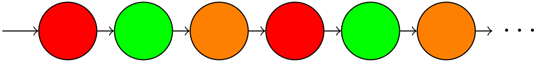
Definition

$$
\begin{aligned}
p &\models a \text{ iff } a \in \ell(p[0]) \\
p &\models f \wedge g \text{ iff } p \models f \wedge p \models g \\
p &\models \neg f \text{ iff } p \not\models f \\
p &\models \bigcirc f \text{ iff } p[1..] \models f \\
p &\models f \,\mathrm{U}\, g \text{ iff } \exists i \geq 0 : p[i..] \models g \wedge \forall 0 \leq j < i : p[j..] \models f
\end{aligned}
$$

LTL

LTL is defined by the grammar

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



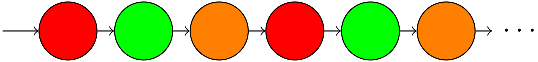
Question

Which LTL formula expresses "initially the light is red and next it becomes green."

LTL

LTL is defined by the grammar

$$f ::= a \mid f \wedge f \mid \neg f \mid \bigcirc f \mid f \; \mathsf{U} \; f$$



Question

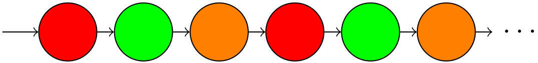
Which LTL formula expresses “initially the light is red and next it becomes green.”

Answer

red $\wedge \bigcirc$green

LTL is defined by the grammar

$$f ::= a \mid f \wedge f \mid \neg f \mid \bigcirc f \mid f \; \mathsf{U} \; f$$



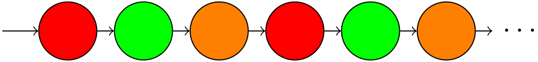
Question

Which LTL formula expresses "the light becomes eventually amber."

LTL

LTL is defined by the grammar

$$f ::= a \mid f \wedge f \mid \neg f \mid \bigcirc f \mid f \mathbin{\mathsf{U}} f$$



Question

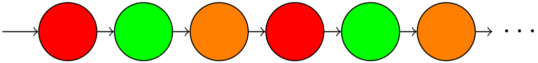
Which LTL formula expresses "the light becomes eventually amber."

Answer

$\Diamond$amber

LTL is defined by the grammar

$$f ::= a \mid f \wedge f \mid \neg f \mid \bigcirc f \mid f \; \mathsf{U} \; f$$



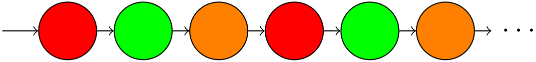
Question

Which LTL formula expresses "the light is infinitely often red."

LTL

LTL is defined by the grammar

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



Question

Which LTL formula expresses "the light is infinitely often red."

Answer

$\Box\Diamond$red

Question

What does the formula $\Box(\text{green} \Rightarrow \neg \bigcirc \text{red})$ express?

LTL

Question

What does the formula $\Box(\text{green} \Rightarrow \neg \bigcirc \text{red})$ express?

Answer

"Once green, the light cannot become red immediately."

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

More practice questions can be found in the textbook.

Equivalence

$\Diamond(f \wedge g) \not\equiv \Diamond f \wedge \Diamond g$

Equivalence

$\Diamond(f \wedge g) \not\equiv \Diamond f \wedge \Diamond g$

For the counter example we provide two ingredients:

- a transition system, and
- LTL formulas for f and g.

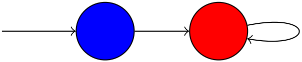
Equivalence

$\Diamond(f \wedge g) \not\equiv \Diamond f \wedge \Diamond g$

For the counter example we provide two ingredients:

- a transition system, and
- LTL formulas for f and g.

Consider the following transition system TS.



Let f = blue and g = red. Then $TS \models \Diamond f \wedge \Diamond g$ but $TS \not\models \Diamond(f \wedge g)$.

Equivalence

$\Diamond \bigcirc f \equiv \bigcirc \Diamond f$

Equivalence

$\Diamond \bigcirc f \equiv \bigcirc \Diamond f$

Proof: Let TS be a transition system. Let $s \in I$ and $p \in Paths(s)$. Then

$$
\begin{aligned}
& p \models \Diamond \bigcirc f \\
& \text{iff } \exists i \geq 0 : p[i..] \models \bigcirc f \\
& \text{iff } \exists i \geq 0 : p[i..][1..] \models f \\
& \text{iff } \exists i \geq 0 : p[(i+1)..] \models f \\
& \text{iff } \exists i \geq 0 : p[1..][i..] \models f \\
& \text{iff } p[1..] \models \Diamond f \\
& \text{iff } p \models \bigcirc \Diamond f
\end{aligned}
$$

Invariants

Definition

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

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

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

$\Box\neg$red

Safety properties

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

Safety properties

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

Question

How can we express this property in LTL?

Answer

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

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

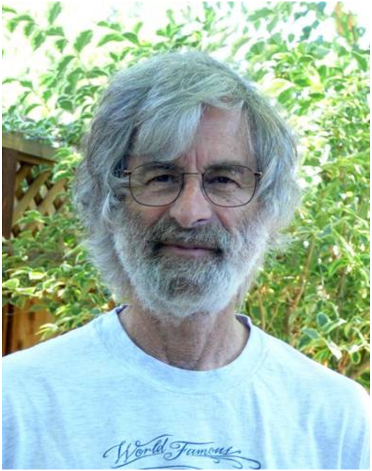
How can we express this property in LTL?

Answer

$\Box\Diamond \mathsf{red}$

Leslie Lamport

- Won the Turing award in 2013.
- Won the Dijkstra prize three times (2000, 2005, 2014).
- Elected Fellow of the ACM in 2014.



Source: Leslie Lamport

Problem

Given a transition system TS and an LTL formula f, check whether $TS \models f$.

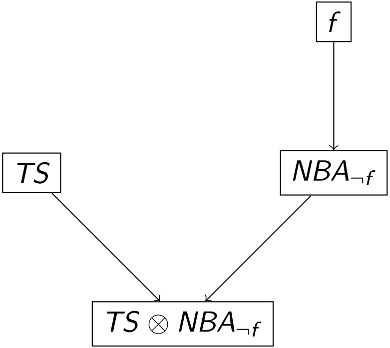
LTL model checking

Problem

Given a transition system TS and an LTL formula f, check whether $TS \models f$.

Algorithm

Given a transition system TS and an LTL formula f, the algorithm returns "yes" if $TS \models f$ and "no" (and a counter example) otherwise.




```
if there exists an accepting run in TS ⊗ NBA¬f
  return ''no''
else
  return ''yes''
```

NBA

Question

What does NBA stand for?

NBA

Question

What does NBA stand for?

Answer

National Basketball Association.

NBA

Question

What does NBA stand for?

Answer

National Basketball Association.

Answer

Nondeterministic Büchi Automaton.

Julius Richard Büchi (1924–1984)

Julius Richard Büchi was a Swiss logician and mathematician.

source: wikipedia

NBA

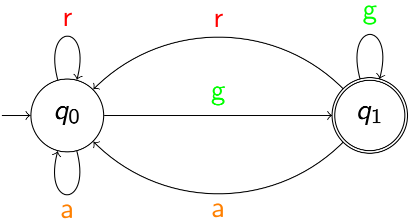
Definition

A nondeterministic Büchi automaton is a tuple $(Q, \Sigma, \delta, I, F)$ consisting of

- a finite set Q of states,
- a finite set Σ of "letters,"
- a transition function $\delta : Q \times \Sigma \to 2^Q$,
- a set I of initial states, and
- a set F of final states.

Σ is called an alphabet.

NBA



Run of an NBA

Definition

The infinite sequence of states $q_0 q_1 q_2 \ldots$ is a run for an infinite sequence of letters $a_0 a_1 a_2 \ldots$ if $q_0 \in I$ and $q_{i+1} \in \delta(q_i, a_i)$ for all $i \geq 0$.

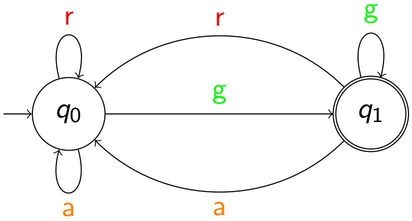
Run of an NBA

Definition

The infinite sequence of states $q_0 q_1 q_2 \ldots$ is a run for an infinite sequence of letters $a_0 a_1 a_2 \ldots$ if $q_0 \in I$ and $q_{i+1} \in \delta(q_i, a_i)$ for all $i \geq 0$.

An infinite sequence of letters is called an (infinite) word.

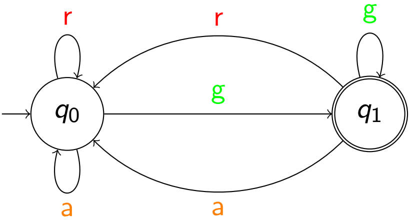
NBA



Question

Is $q_0 q_1 q_0 q_1 q_0 q_1 \ldots$ a run for g a g r g a $\ldots$?

NBA



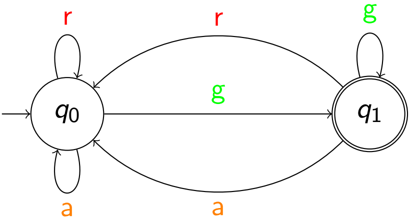
Question

Is $q_0 q_1 q_0 q_1 q_0 q_1 \ldots$ a run for g a g r g a $\ldots$?

Answer

Yes.

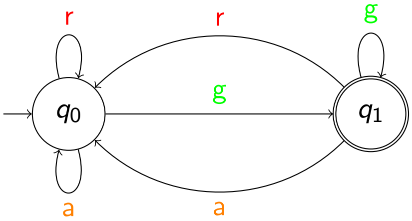
NBA



Question

Is $q_0 q_1 q_0 q_1 q_0 q_1 \ldots$ a run for g r g r g r . . . ?

NBA



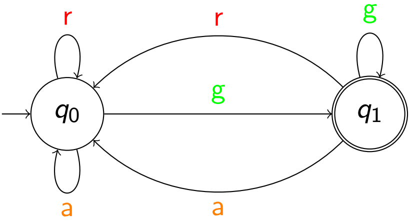
Question

Is $q_0 q_1 q_0 q_1 q_0 q_1 \ldots$ a run for g r g r g r ...?

Answer

Yes.

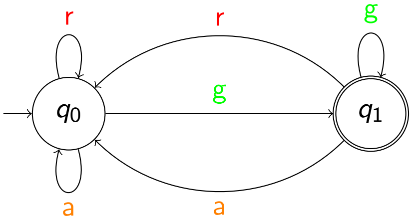
NBA



Question

Is $q_0 q_0 q_0 q_0 q_0 q_0 \ldots$ a run for r a r a r a ...?

NBA



Question

Is $q_0 q_0 q_0 q_0 q_0 q_0 \ldots$ a run for r a r a r a $\ldots$?

Answer

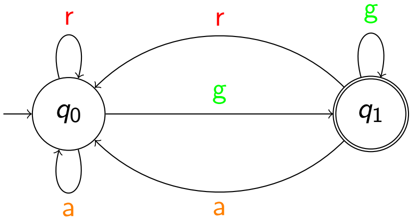
Yes.

Accepting run of an NBA

Definition

A run $q_0 q_1 q_2 \ldots$ is accepting if $q_i \in F$ for infinitely many $i \geq 0$.

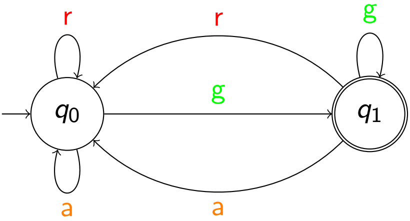
NBA



Question

Is the run $q_0 q_1 q_0 q_1 q_0 q_1 \ldots$ accepting?

NBA



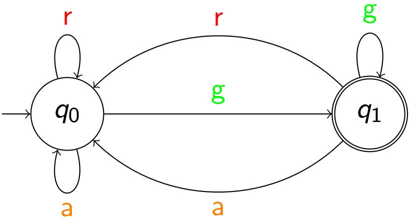
Question

Is the run $q_0 q_1 q_0 q_1 q_0 q_1 \ldots$ accepting?

Answer

Yes.

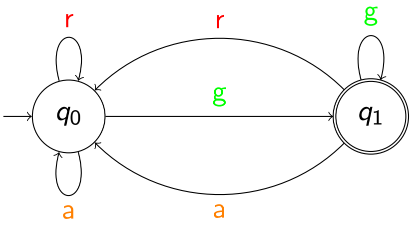
NBA



Question

Is the run $q_0 q_0 q_0 q_0 q_0 q_0 \ldots$ accepting?

NBA



Question

Is the run $q_0 q_0 q_0 q_0 q_0 q_0 \ldots$ accepting?

Answer

No.

Words and LTL formulas

Definition

Let w be a word.

$$
\begin{aligned}
w \models a &\text{ iff } a = w[0] \\
w \models f \wedge g &\text{ iff } w \models f \wedge w \models g \\
w \models \neg f &\text{ iff } w \not\models f \\
w \models \bigcirc f &\text{ iff } w[1..] \models f \\
w \models f \,\mathsf{U}\, g &\text{ iff } \exists i \geq 0 : w[i..] \models g \wedge \forall 0 \leq j < i : w[j..] \models f
\end{aligned}
$$

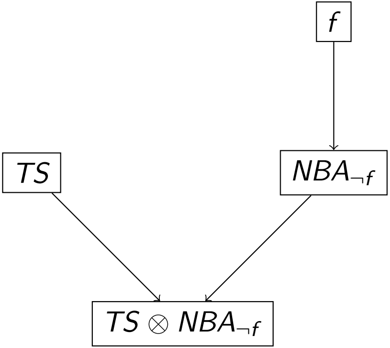
For each LTL formula f, there exists an NBA such that it has an accepting run for w if and only if $w \models f$.

LTL formulas and NBAs

For each LTL formula f, there exists an NBA such that it has an accepting run for w if and only if $w \models f$.

The NBA on slide 20 corresponds to the LTL formula $\Box\Diamond g$. Note that its negation is equivalent to $\Diamond\Box\neg g$.

Overview of algorithm



`if there exists an accepting run in` $TS \otimes NBA_{\neg f}$
  `return ‘‘no’’`
`else`
  `return ‘‘yes’’`

Further details can be found in the textbook.

Expressiveness of LTL

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 f with $TS \models f$ iff

$$\forall s \in I : \forall p \in Paths(s) : \forall m \geq 0 : \exists q \in Paths(p[m]) : \exists n \geq 0 : q[n] \models a$$

How to modify the logic?

$$\forall s \in I : \forall p \in Paths(s) : \forall m \geq 0 : \exists q \in Paths(p[m]) : \underbrace{\exists n \geq 0 : q[n] \models a}_{\Diamond a}$$

How to modify the logic?

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

How to modify the logic?

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

How to modify the logic?

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

How to modify the logic?

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

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

Question

$? \models \exists \Diamond a$.

How to modify the logic?

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

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?

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

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*.

Computational Tree Logic

EECS 4315

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

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

$$g ::= \bigcirc f \mid f \; \mathsf{U} \; f$$

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

$$g ::= \bigcirc f \mid f \; \mathsf{U} \; f$$

The *formulas* are defined by

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

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.

Syntactic sugar

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

Semantics of CTL

$$\begin{array}{rcl} s \models a & \text{iff} & a \in \ell(s) \\ s \models f_1 \wedge f_2 & \text{iff} & s \models f_1 \wedge s \models f_2 \\ s \models \neg f & \text{iff} & s \not\models f \\ s \models \exists g & \text{iff} & \exists p \in Paths(s) : p \models g \\ s \models \forall g & \text{iff} & \forall p \in Paths(s) : p \models g \end{array}$$

and

$$\begin{array}{rcl} p \models \bigcirc f & \text{iff} & p[1] \models f \\ p \models f_1 \, \mathsf{U} \, f_2 & \text{iff} & \exists i \geq 0 : p[i] \models f_2 \wedge \forall 0 \leq j < i : p[j] \models f_1 \end{array}$$