Model Checking

Lecture #7: Linear Temporal Logic

[Baier & Katoen, Chapter 5.1]

Joost-Pieter Katoen

Software Modeling and Verification Group

Model Checking Course, RWTH Aachen, WiSe 2019/2020

Overview

Overview

Specifying LT Properties

- An LT property is a set of infinite traces over AP
- Specifying such sets explicitly is often inconvenient
- Mutual exclusion is specified over $AP = \{ c_1, c_2 \}$ by

  E_{mutex} = set of infinite words $A_0 \, A_1 \ldots$ with $\{ c_1, c_2 \} \not\subseteq A_i$ for all $0 \leq i$

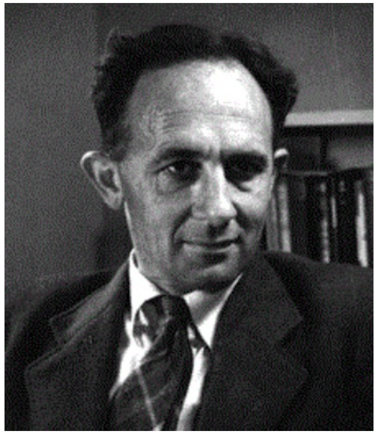
- Starvation freedom is specified over $AP = \{ c_1, w_1, c_2, w_2 \}$ by

  $E_{nostarve}$ = set of infinite words $A_0 \, A_1 \ldots$ such that:

$$\left(\overset{\infty}{\exists} j.\ w_1 \in A_j \right) \Rightarrow \left(\overset{\infty}{\exists} j.\ c_1 \in A_j \right) \wedge \left(\overset{\infty}{\exists} j.\ w_2 \in A_j \right) \Rightarrow \left(\overset{\infty}{\exists} j.\ c_2 \in A_j \right)$$

Such properties can be specified much more succinctly using logic (or using ω-regular expressions)

Linear Temporal Logic



Arthur Norman Prior
(1914–†1969)

Amir Pnueli
(1941–†2009)

LTL Syntax

Definition: LTL syntax

BNF grammar for LTL formulas with proposition $a \in AP$:

$$\varphi ::= \text{true} \;\big|\; a \;\big|\; \varphi_1 \wedge \varphi_2 \;\big|\; \neg\varphi \;\big|\; \bigcirc\varphi \;\big|\; \varphi_1 \,\mathsf{U}\, \varphi_2$$

- Propositional logic
  - $a \in AP$ — atomic proposition
  - $\neg\varphi$ and $\varphi \wedge \psi$ — negation and conjunction
- Temporal modalities
  - $\bigcirc\varphi$ — neXt state fulfills φ
  - $\varphi \,\mathsf{U}\, \psi$ — φ holds Until a ψ-state is reached

Linear Temporal Logic (LTL) is a logic to describe LT properties

Derived Operators

$$\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$$

$$\varphi \Rightarrow \psi \equiv \neg\varphi \vee \psi$$

$$\varphi \Leftrightarrow \psi \equiv (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$$

$$\varphi \oplus \psi \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$$

$$\text{true} \equiv \varphi \vee \neg\varphi$$

$$\text{false} \equiv \neg\,\text{true}$$

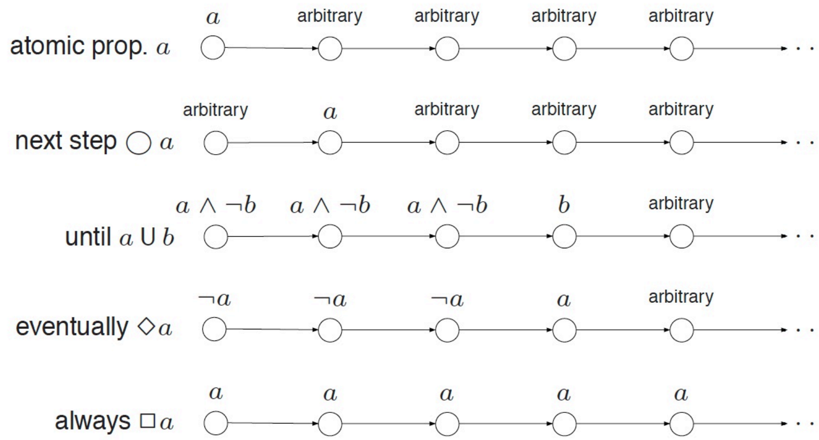
$\Diamond\varphi \equiv \text{true}\,\mathsf{U}\,\varphi$ "some time in the future"

$\Box\varphi \equiv \neg\Diamond\neg\varphi$ "from now on forever"

precedence order: the unary operators bind stronger than the binary ones.

$\neg$ and $\bigcirc$ bind equally strong. U takes precedence over $\wedge$, $\vee$, and $\Rightarrow$

Intuitive Semantics



Example: Traffic Light Properties

- Once red, the light cannot become green immediately:

$$\Box(red \Rightarrow \neg \bigcirc green)$$

- The green light becomes green eventually: $\Diamond green$

- Once red, the light becomes green eventually: $\Box(red \Rightarrow \Diamond green)$

- Once red, the light always becomes green eventually after being yellow for some time inbetween:

$$\Box\big(red \rightarrow \bigcirc(red \,\mathsf{U}\, (yellow \wedge \bigcirc(yellow \,\mathsf{U}\, green)))\big)$$

Example Properties in LTL

- Reachability
  - negated reachability $\Diamond \neg \psi$
  - conditional reachability $\varphi \,\mathsf{U}\, \psi$
  - reachability from any state not expressible
- Safety
  - simple safety $\Box \neg \varphi$
  - conditional safety $(\varphi \,\mathsf{U}\, \psi) \vee \Diamond \varphi$
- Liveness $\Box(\varphi \Rightarrow \Diamond \psi)$ and others

Overview

Semantics Over Words

Definition: LTL semantics over infinite words

The LT-property induced by LTL formula φ over AP is:

$$Words(\varphi) = \left\{ \sigma \in \left(2^{AP}\right)^{\omega} \mid \sigma \models \varphi \right\}, \text{ where } \models \text{ is the smallest relation with:}$$

$$
\begin{array}{lcl}
\sigma \models \text{true} & & \\
\sigma \models a & \text{iff} & a \in A_0 \quad (\text{i.e., } A_0 \models a) \\
\sigma \models \varphi_1 \wedge \varphi_2 & \text{iff} & \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2 \\
\sigma \models \neg \varphi & \text{iff} & \sigma \not\models \varphi \\
\sigma \models \bigcirc \varphi & \text{iff} & \sigma[1..] = A_1 A_2 A_3 \ldots \models \varphi \\
\sigma \models \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \exists j \geq 0.\ \sigma[j..] \models \varphi_2 \text{ and } \sigma[i..] \models \varphi_1,\ 0 \leq i < j
\end{array}
$$

for $\sigma = A_0 A_1 A_2 \ldots$, let $\sigma[i..] = A_i A_{i+1} A_{i+2} \ldots$ be the suffix of σ from index i on.

Semantics of $\Box$, $\Diamond$, $\Box\Diamond$ and $\Diamond\Box$

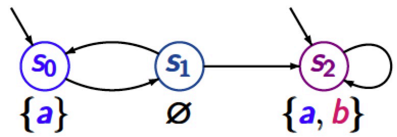
$\sigma \models \Diamond\varphi$ iff $\exists j \geq 0.\ \sigma[j..] \models \varphi$

$\sigma \models \Box\varphi$ iff $\forall j \geq 0.\ \sigma[j..] \models \varphi$

$\sigma \models \Box\Diamond\varphi$ iff $\forall j \geq 0.\ \exists i \geq j.\ \sigma[i\ldots] \models \varphi$

$\sigma \models \Diamond\Box\varphi$ iff $\exists j \geq 0. \forall i \geq j.\ \sigma[i\ldots] \models \varphi$

Example



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\,\varnothing\,\{a,b\}^\omega$

$\pi \models a$, but $\pi \not\models b$	as $L(s_0) = \{a\}$
$\pi \models \bigcirc(\neg a \wedge \neg b)$	as $L(s_1) = \varnothing$
$\pi \models \bigcirc\bigcirc(a \wedge b)$	as $L(s_2) = \{a, b\}$
$\pi \models (\neg b)\ \mathsf{U}\ (a \wedge b)$	as $s_0, s_1 \models \neg b$
$\pi \models (\neg b)\ \mathsf{U}\ \Box(a \wedge b)$	and $s_2 \models a \wedge b$

Semantics over Paths and States

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system and φ be an LTL-formula over AP.

- For infinite path fragment π of TS:

$$\pi \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

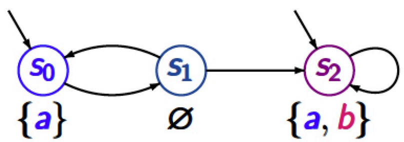
- For state $s \in S$:

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

- For transition system TS:

$$TS \models \varphi \quad \text{iff} \quad Traces(TS) \subseteq Words(\varphi) \quad \text{iff} \quad \forall s \in I.\ s \models \varphi$$

Example



$AP = \{a, b\}$

$\mathcal{T} \models a$	as $s_0 \models a$ and $s_2 \models a$
$\mathcal{T} \not\models \Diamond\Box a$	as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$
$\mathcal{T} \models \Diamond\Box b \vee \Box\Diamond(\neg a \wedge \neg b)$	as $s_2 \models b$, $s_1 \not\models a, b$
$\mathcal{T} \models \Box(a \rightarrow (\bigcirc\neg a \vee b))$	as $s_2 \models b$, $s_0 \models \bigcirc\neg a$

On The Semantics of Negation

For paths, it holds $\pi \models \varphi$ if and only if $\pi \not\models \neg\varphi$ since:

$$Words(\neg\varphi) = \left(2^{AP}\right)^{\omega} \setminus Words(\varphi) \quad .$$

But: $TS \not\models \varphi$ and $TS \models \neg\varphi$ are *not* equivalent in general

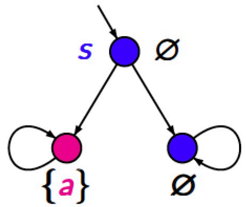
It holds: $TS \models \neg\varphi$ implies $TS \not\models \varphi$. Not always the reverse!

Note that:

$$\begin{aligned} TS \not\models \varphi \quad & \text{iff} \quad Traces(TS) \not\subseteq Words(\varphi) \\ & \text{iff} \quad Traces(TS) \setminus Words(\varphi) \neq \varnothing \\ & \text{iff} \quad Traces(TS) \cap Words(\neg\varphi) \neq \varnothing \quad . \end{aligned}$$

TS neither satisfies φ nor $\neg\varphi$ if there are paths π_1 and π_2 in TS such that $\pi_1 \models \varphi$ and $\pi_2 \models \neg\varphi$

Example



$s \not\models \Diamond a$ and $s \not\models \neg\Diamond a$

LTL Formulas for LT Properties

Provide LTL formulas over $AP = \{ a, b \}$ for the LT properties:

- set of all words $A_0 A_1 \ldots$ over $\left(2^{AP}\right)^{\omega}$ such that:

$$\begin{aligned} & \forall i \geq 0. \left(a \in A_i \;\Rightarrow\; i > 0 \,\wedge\, b \in A_{i-1}\right) \\ \equiv\; & \forall j \geq 0. \left(b \in A_j \,\vee\, a \notin A_{j+1}\right) \\ \equiv\; & Words(\Box(b \vee \neg\bigcirc a)) \end{aligned}$$

- set of all words of the form

$$\{ b \}^{n_1} \{ a \} \{ b \}^{n_2} \{ a \} \{ b \}^{n_3} \{ a \} \ldots$$

where $n_i \geq 0$. This is captured by

$$Words(\Box((b \wedge \neg a) \,\mathsf{U}\, (a \wedge \neg b)))$$

Overview

LTL Equivalence

Definition: LTL equivalence

LTL formulas φ, ψ (both over AP) are equivalent:

$$\varphi \equiv_{LTL} \psi \quad \text{if and only if} \quad Words(\varphi) = Words(\psi).$$

If it is clear from the context that we deal with LTL-formulas, we simply write $\varphi \equiv \psi$.

Equivalently:

$$\varphi \equiv_{LTL} \psi \text{ iff } \big(\text{for all transition systems } TS: TS \models \varphi \text{ iff } TS \models \psi \big).$$

Duality and Idempotence

Duality:

$$\neg \Box \varphi \equiv \Diamond \neg \varphi$$
$$\neg \Diamond \varphi \equiv \Box \neg \varphi$$
$$\neg \bigcirc \varphi \equiv \bigcirc \neg \varphi$$

Idempotence:

$$\Box \Box \varphi \equiv \Box \varphi$$
$$\Diamond \Diamond \varphi \equiv \Diamond \varphi$$
$$\varphi \, \mathsf{U} \, (\varphi \, \mathsf{U} \, \psi) \equiv \varphi \, \mathsf{U} \, \psi$$
$$(\varphi \, \mathsf{U} \, \psi) \, \mathsf{U} \, \psi \equiv \varphi \, \mathsf{U} \, \psi$$

Absorption and Distributive

Absorption:

$$\Diamond \Box \Diamond \varphi \equiv \Box \Diamond \varphi$$
$$\Box \Diamond \Box \varphi \equiv \Diamond \Box \varphi$$

Distributive:

$$\bigcirc (\varphi \, \mathsf{U} \, \psi) \equiv (\bigcirc \varphi) \, \mathsf{U} \, (\bigcirc \psi)$$
$$\Diamond(\varphi \vee \psi) \equiv \Diamond \varphi \vee \Diamond \psi$$
$$\Box(\varphi \wedge \psi) \equiv \Box \varphi \wedge \Box \psi$$

but ......:

$$\Diamond(\varphi \, \mathsf{U} \, \psi) \not\equiv (\Diamond \varphi) \, \mathsf{U} \, (\Diamond \psi)$$
$$\Diamond(\varphi \wedge \psi) \not\equiv \Diamond \varphi \wedge \Diamond \psi$$
$$\Box(\varphi \vee \psi) \not\equiv \Box \varphi \vee \Box \psi$$

Expansion Law

Expansion:

$$\varphi \, \mathsf{U} \, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \, \mathsf{U} \, \psi))$$
$$\Diamond \varphi \equiv \varphi \vee \bigcirc \Diamond \varphi$$
$$\Box \varphi \equiv \varphi \wedge \bigcirc \Box \varphi$$

Proof.

On the black board. Expansion laws can have multiple solutions. □

Expansion for Until

$Words(\varphi \, U \, \psi)$ is the smallest LT-property P such that:

1. $Words(\psi) \subseteq P$, and
2. $\{A_0 A_1 A_2 \ldots \in Words(\varphi) \mid A_1 A_2 \ldots \in P\} \subseteq P$

where smallest is w.r.t. the $\subseteq$-ordering on sets (of infinite words).

Equivalently, $Words(\varphi \, U \, \psi)$ is the smallest LT property P such that:

$$Words(\psi) \cup \{A_0 A_1 A_2 \ldots \in Words(\varphi) \mid A_1 A_2 \ldots \in P\} \subseteq P.$$

Proof

Weak Until

Definition: the weak-until-operator

The weak-until (or: unless) operator is defined by

$$\varphi \, W \, \psi \; = \; (\varphi \, U \, \psi) \lor \Box \varphi.$$

In contrast to until, weak until does not require to establish ψ eventually

Until U and weak until W are dual:

$$\neg(\varphi \, U \, \psi) \equiv (\varphi \land \neg\psi) \, W \, (\neg\varphi \land \neg\psi)$$

$$\neg(\varphi \, W \, \psi) \equiv (\varphi \land \neg\psi) \, U \, (\neg\varphi \land \neg\psi)$$

Example

Expansion for Weak Until

Recall: $Words(\varphi \,\mathsf{U}\, \psi)$ is the smallest LT property P such that

$$Words(\psi) \cup \{A_0 A_1 A_2 \ldots \in Words(\varphi) \mid A_1 A_2 \ldots \in P\} \subseteq P.$$

$Words(\varphi \,\mathsf{W}\, \psi)$ is the largest LT-property P such that:

$$Words(\psi) \cup \{A_0 A_1 A_2 \ldots \in Words(\varphi) \mid A_1 A_2 \ldots \in P\} \supseteq P$$

where largest is w.r.t. the $\subseteq$ ordering on sets (of infinite words).

Overview

The Release Operator

Definition: release operator

The release operator is defined by

$$\varphi \,\mathsf{R}\, \psi \;=\; \neg(\neg\varphi \,\mathsf{U}\, \neg\psi)\,.$$

Semantics:

$$\sigma \models \varphi \,\mathsf{R}\, \psi \quad \text{iff} \quad \sigma \models \Box\psi \;\vee\; \exists i.\, (\sigma[i..] \models \varphi \wedge \forall k \leq i. \sigma[k..] \models \psi)$$

ψ always holds, a requirements that is released once φ becomes valid
It follows:

$$\Box\varphi \;\equiv\; \mathit{false}\,\mathsf{R}\,\varphi$$
$$\varphi \,\mathsf{W}\, \psi \;\equiv\; (\neg\varphi \vee \psi)\,\mathsf{R}\,(\varphi \vee \psi)$$
$$\varphi \,\mathsf{R}\, \psi \;\equiv\; \psi \wedge (\varphi \vee \bigcirc(\varphi \,\mathsf{R}\, \psi))$$

The Semantics of Release

$\sigma \models \varphi \,\mathsf{R}\, \psi$

iff (* definition of R *)

$\sigma \models \neg(\neg\varphi \,\mathsf{U}\, \neg\psi)$

iff (* definition of U *)

$\neg\exists j \geq 0.\, (\sigma[j..] \models \neg\psi \wedge \forall i < j.\, \sigma[i..] \models \neg\varphi)$

iff (* semantics of negation *)

$\neg\exists j \geq 0.\, (\sigma[j..] \not\models \psi \;\wedge\; \forall i < j.\, \sigma[i..] \not\models \varphi)$

iff (* duality of $\exists$ and $\forall$ *)

$\forall j \geq 0.\, \neg\big(\sigma[j..] \not\models \psi \;\wedge\; \forall i < j.\, \sigma[i..] \not\models \varphi\big)$

iff (* de Morgan's law *)

$\forall j \geq 0.\, \big(\neg(\sigma[j..] \not\models \psi) \;\vee\; \neg\forall i < j.\, \sigma[i..] \not\models \varphi\big)$

iff (* semantics of negation *)

$\forall j \geq 0.\, \big(\sigma[j..] \models \psi \;\vee\; \exists i < j.\, \sigma[i..] \models \varphi\big)$

iff

$\forall j \geq 0.\, \sigma[j..] \models \psi$ **or** $(\exists i \geq 0.\, (\sigma[i..] \models \varphi) \wedge \forall k \leq i.\, \sigma[k..] \models \psi)$

Positive Normal Form

Definition: positive normal form

The LTL-formula φ is in positive normal form (PNF) if it is of the form:

$$\varphi ::= \text{true} \mid \text{false} \mid a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \bigcirc \varphi \mid \varphi_1 \mathsf{U} \varphi_2 \mid \varphi_1 \mathsf{R} \varphi_2.$$

As $\Box\varphi \equiv \text{false} \mathsf{R} \varphi$, $\Box\varphi$ is in PNF; $\Diamond \varphi \equiv \text{true} \mathsf{U} \varphi$ is in PNF too.

For each LTL-formula φ, there exists an equivalent LTL-formula ψ in PNF such that $|\psi| \in O(|\varphi|)$.

Proof.

Transformation rules to push negations into the LTL-formula φ, in particular $\neg \bigcirc \varphi \equiv \bigcirc \neg\varphi$ and $\neg(\varphi \mathsf{U} \psi) \equiv \neg\varphi \mathsf{R} \neg\psi$. □

Overview

Summary

- Linear temporal logic (LTL) is a logic to succinctly describe LT properties
- LTL-formulas are equivalent iff they describe the same LT properties
- The until-operator is the smallest solution of an expansion law
- The weak until-operator is the largest solution of that expansion law
- An LTL-formula is in positive normal form if negations only occur adjacent to propositions
- Each LTL-formula can be transformed into an equivalent LTL-formula in PNF

Next Lecture

Thursday November 14, 10:30