Linear Temporal Logic

Lecture #13 of Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

E-mail: `katoen@cs.rwth-aachen.de`

December 2, 2008

Overview Lecture #12

- Syntax
- Semantics
- Equivalence

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

$$P_{mutex} \;=\; \text{set of infinite words } A_0\, A_1\, A_2 \ldots \text{ with } \{ c_1, c_2 \} \not\subseteq A_i \text{ for all } 0 \leqslant i$$

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

$$P_{nostarve} \;=\; \text{set of infinite words } A_0\, A_1\, A_2 \ldots \text{ such that:}$$

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

such properties can be specified succinctly using logic

Syntax

modal logic over infinite sequences [Pnueli 1977]

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

linear temporal logic is a logic for describing LT properties

Derived operators

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

$$\phi \Rightarrow \psi \equiv \neg\phi \vee \psi$$

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

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

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

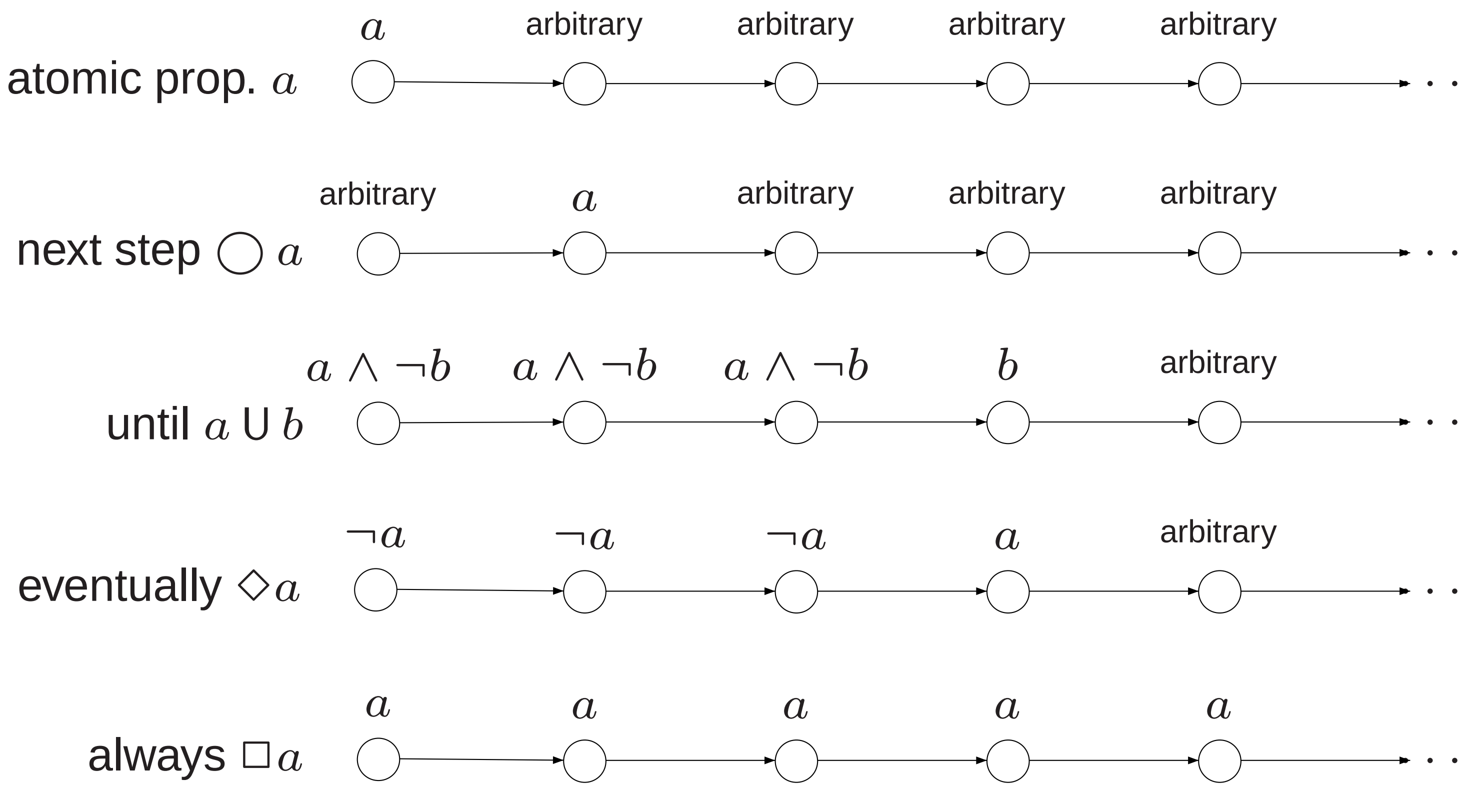
$$\text{false} \equiv \neg\,\text{true}$$

$$\Diamond\phi \equiv \text{true}\ \mathsf{U}\ \phi \qquad \text{“sometimes in the future”}$$

$$\Box\phi \equiv \neg\Diamond\neg\phi \qquad \text{“from now on for ever”}$$

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



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:

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

Practical properties in LTL

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

Semantics over words

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

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

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

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

Semantics of □, ◇, □◇ and ◇□

$$\sigma \models \Diamond\varphi \quad \text{iff} \quad \exists j \geqslant 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geqslant 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\Diamond\varphi \quad \text{iff} \quad \forall j \geqslant 0. \exists i \geqslant j.\ \sigma[i \ldots] \models \varphi$$

$$\sigma \models \Diamond\Box\varphi \quad \text{iff} \quad \exists j \geqslant 0. \forall j \geqslant i.\ \sigma[j \ldots] \models \varphi$$

Semantics over paths and states

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

- For infinite path fragment π of *TS*:

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

- For state $s \in S$:

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

- *TS* satisfies φ, denoted *TS* $\models \varphi$, iff $\mathit{Traces}(\mathit{TS}) \subseteq \mathit{Words}(\varphi)$

Semantics for transition systems

$TS \models \varphi$

iff (* transition system semantics *)

$\mathit{Traces}(\mathit{TS}) \subseteq \mathit{Words}(\varphi)$

iff (* definition of $\models$ for LT-properties *)

$\mathit{TS} \models \mathit{Words}(\varphi)$

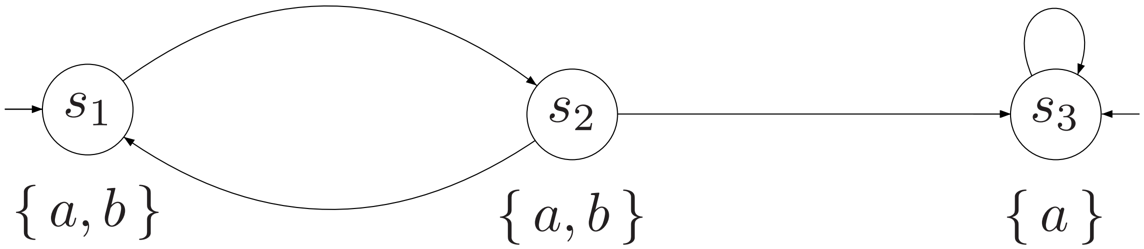
iff (* Definition of $\mathit{Words}(\varphi)$ *)

$\pi \models \varphi$ for all $\pi \in \mathit{Paths}(\mathit{TS})$

iff (* semantics of $\models$ for states *)

$s_0 \models \varphi$ for all $s_0 \in I$.

Example



$$TS \models \Box a \quad TS \not\models \bigcirc (a \wedge b)$$

$$TS \models \Box(\neg b \;\Rightarrow\; \Box(a \wedge \neg b)) \quad TS \not\models b \,\mathsf{U}\, (a \wedge \neg b)$$

Semantics of negation

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

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

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

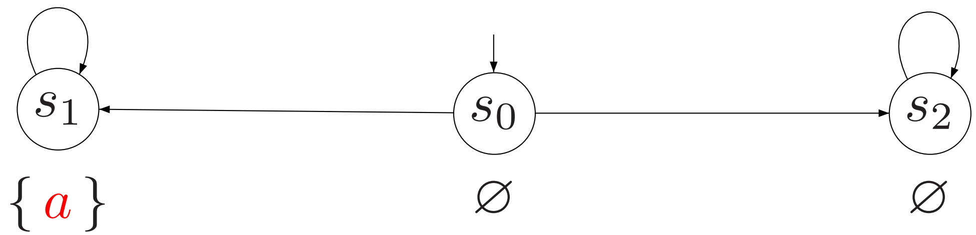
It holds: $TS \models \neg\varphi$ implies $TS \not\models \varphi$. Not always the reverse!

Note that:

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

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



A transition system for which *TS* $\not\models \Diamond a$ and *TS* $\not\models \neg\Diamond a$

Specifying properties in LTL

Equivalence

LTL formulas ϕ, ψ are *equivalent*, denoted $\phi \equiv \psi$, if:

$$\textit{Words}(\phi) = \textit{Words}(\psi)$$

Duality and idempotence laws

Duality:

$$\neg \Box \phi \equiv \Diamond \neg \phi$$

$$\neg \Diamond \phi \equiv \Box \neg \phi$$

$$\neg \bigcirc \phi \equiv \bigcirc \neg \phi$$

Idempotency:

$$\Box \Box \phi \equiv \Box \phi$$

$$\Diamond \Diamond \phi \equiv \Diamond \phi$$

$$\phi \,\mathsf{U}\, (\phi \,\mathsf{U}\, \psi) \equiv \phi \,\mathsf{U}\, \psi$$

$$(\phi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \psi \equiv \phi \,\mathsf{U}\, \psi$$

Absorption and distributive laws

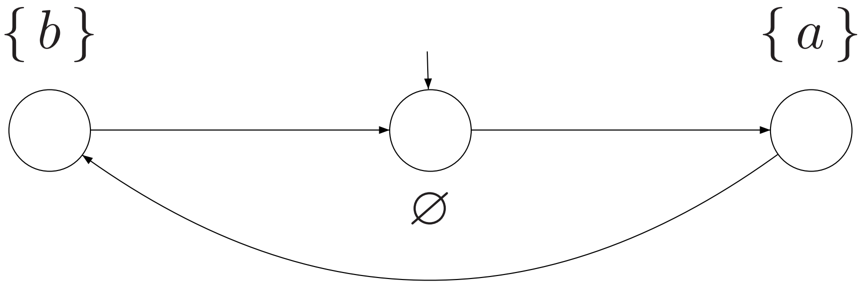
Absorption:
$$\Diamond \Box \Diamond \phi \equiv \Box \Diamond \phi$$
$$\Box \Diamond \Box \phi \equiv \Diamond \Box \phi$$

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

but . . . . . .:
$$\Diamond(\phi \,\mathsf{U}\, \psi) \not\equiv (\Diamond\phi) \,\mathsf{U}\, (\Diamond\psi)$$
$$\Diamond(\phi \wedge \psi) \not\equiv \Diamond\phi \wedge \Diamond\psi$$
$$\Box(\phi \vee \psi) \not\equiv \Box\phi \vee \Box\psi$$

Distributive laws

$$\Diamond(a \wedge b) \not\equiv \Diamond a \ \wedge \ \Diamond b \quad \text{and} \quad \Box(a \ \vee \ b) \not\equiv \Box a \ \ \vee \ \ \Box b$$



$TS \not\models \Diamond(a \wedge b)$ and $TS \models \Diamond a \ \wedge \ \Diamond b$