Linear Temporal Logic (2)

Lecture #13 of Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

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

May 16, 2007

Overview Lecture #13

$\Rightarrow$ Repetition: LTL syntax and semantics

- LTL equivalence
- Expansion laws
- Positive normal form

Linear temporal logic

BNF grammar for LTL formulas over propositions *AP* with $a \in$ *AP*:

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

auxiliary temporal operators: $\Diamond\, \phi \equiv \text{true}\, \mathsf{U}\, \phi$ and $\Box\, \phi \equiv \neg \Diamond \neg\, \phi$

LTL semantics

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:

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

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 $\Box$, $\Diamond$, $\Box\Diamond$ and $\Diamond\Box$

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

LTL semantics

Let $\mathit{TS} = (S, \mathit{Act}, \longrightarrow, I, \mathit{AP}, L)$ be a transition system without terminal states, and let 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 $\mathit{TS} \models \varphi$, if $\mathit{Traces}(\mathit{TS}) \subseteq \mathit{Words}(\varphi)$

Overview Lecture #13

- Repetition: LTL syntax and semantics

⇒ LTL equivalence

- Expansion laws

- Positive normal form

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:

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

$$\Diamond(\phi \lor \psi) \equiv \Diamond\phi \lor \Diamond\psi$$

$$\Box(\phi \land \psi) \equiv \Box\phi \land \Box\psi$$

but . . . . . .:

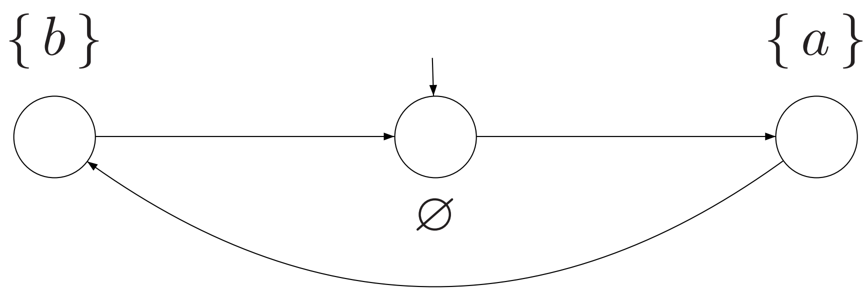
$$\Diamond(\phi \,\mathsf{U}\, \psi) \not\equiv (\Diamond\phi) \,\mathsf{U}\, (\Diamond\psi)$$

$$\Diamond(\phi \land \psi) \not\equiv \Diamond\phi \land \Diamond\psi$$

$$\Box(\phi \lor \psi) \not\equiv \Box\phi \lor \Box\psi$$

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* $\models \Diamond a \wedge \Diamond b$

Overview Lecture #13

- Repetition: LTL syntax and semantics
- LTL equivalence

$\Rightarrow$ Expansion laws

- Positive normal form

Expansion laws

Expansion:

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

$$\Diamond \phi \equiv \phi \vee \bigcirc \Diamond \phi$$

$$\Box \phi \equiv \phi \wedge \bigcirc \Box \phi$$

proof on the black board

Expansion for until

$P = \textit{Words}(\varphi \,\mathsf{U}\, \psi)$ satisfies:

$$P \;=\; \textit{Words}(\psi) \cup \{\, A_0A_1A_2\ldots \in \textit{Words}(\varphi) \;\mid\; A_1A_2\ldots \in P \,\}$$

and is the *smallest* LT-property such that:

$$\textit{Words}(\psi) \cup \{A_0A_1A_2\ldots \in \textit{Words}(\varphi) \;\mid\; A_1A_2\ldots \in P\} \;\subseteq\; P \qquad (*)$$

smallest LT-property satisfying condition (*) means that:
$P = \textit{Words}(\varphi \,\mathsf{U}\, \psi)$ satisfies (*) and $\textit{Words}(\varphi \,\mathsf{U}\, \psi) \subseteq P$ for each P satisfying (*)

Proof

Weak until

- The *weak-until* (or: unless) operator: $\varphi \, \mathsf{W} \, \psi \overset{\text{def}}{=} (\varphi \, \mathsf{U} \, \psi) \lor \Box\varphi$
  - as opposed to until, $\varphi \, \mathsf{W} \, \psi$ does not require a ψ-state to be reached

- Until U and weak until W are *dual*:

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

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

- Until and weak until are *equally expressive*:
  - $\Box\psi \equiv \psi \, \mathsf{W} \, \text{false}$ and $\varphi \, \mathsf{U} \, \psi \equiv (\varphi \, \mathsf{W} \, \psi) \land \neg\Box\neg\psi$

- Until and weak until satisfy the *same expansion law*
  - but until is the smallest, and weak until the largest solution!

Expansion for weak until

$P = \mathit{Words}(\varphi \, \mathsf{W} \, \psi)$ satisfies:

$$P \;=\; \mathit{Words}(\psi) \cup \{\, A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \;\mid\; A_1 A_2 \ldots \in P \,\}$$

and is the *largest* LT-property such that:

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

largest LT-property satisfying condition (**) means that:

$P \supseteq \mathit{Words}(\varphi \, \mathsf{W} \, \psi)$ satisfies (**) and $\mathit{Words}(\varphi \, \mathsf{W} \, \psi) \supseteq P$ for each P satisfying (**)

Overview Lecture #13

- Repetition: LTL syntax and semantics
- LTL equivalence
- Expansion laws

$\Rightarrow$ Positive normal form

(Weak-until) positive normal form

- Canonical form for LTL-formulas
  - negations only occur adjacent to atomic propositions
  - disjunctive and conjunctive normal form is a special case of PNF
  - for each LTL-operator, a dual operator is needed
  - e.g., $\neg(\varphi \,\mathsf{U}\, \psi) \;\equiv\; \big((\varphi \wedge \neg\psi) \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)\big) \;\vee\; \Box(\varphi \wedge \neg\psi)$
  - that is: $\neg(\varphi \,\mathsf{U}\, \psi) \;\equiv\; (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi)$

- For $a \in AP$, the set of LTL formulas in PNF is given by:

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

  - $\Box$ and $\Diamond$ are also permitted: $\Box\varphi \equiv \varphi \,\mathsf{W}\, \text{false}$ and $\Diamond\varphi = \text{true} \,\mathsf{U}\, \varphi$

(Weak until) PNF is always possible

For each LTL-formula there exists an equivalent LTL-formula in PNF

Transformations:

$$
\begin{array}{lcl}
\neg \text{true} & \rightsquigarrow & \text{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi \wedge \psi) & \rightsquigarrow & \neg\varphi \vee \neg\psi \\
\neg(\varphi \vee \psi) & \rightsquigarrow & \neg\varphi \wedge \neg\psi \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc \neg\varphi \\
\neg(\varphi \, \mathsf{U} \, \psi) & \rightsquigarrow & (\varphi \wedge \neg\psi) \, \mathsf{W} \, (\neg\varphi \wedge \neg\psi) \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \\
\neg\Box\varphi & \rightsquigarrow & \Diamond\neg\varphi
\end{array}
$$

but an exponential growth in size is possible

Example

Consider the LTL-formula $\neg\Box\big((a \,\mathsf{U}\, b) \;\vee\; \bigcirc\, c\big)$

This formula is not in PNF, but can be transformed into PNF as follows:

$$
\begin{aligned}
& \neg\Box\big((a \,\mathsf{U}\, b) \;\vee\; \bigcirc\, c\big) \\
\equiv\; & \Diamond\neg\big((a \,\mathsf{U}\, b) \;\vee\; \bigcirc\, c\big) \\
\equiv\; & \Diamond\big(\neg(a \,\mathsf{U}\, b) \wedge \neg \bigcirc\, c\big) \\
\equiv\; & \Diamond\big((a \wedge \neg b) \,\mathsf{W}\, (\neg a \wedge \neg b) \;\wedge\; \bigcirc\, \neg c\big)
\end{aligned}
$$

can the exponential growth in size be avoided?

The release operator

- The *release* operator: $\varphi \, \mathsf{R} \, \psi \ \stackrel{\text{def}}{=} \ \neg(\neg\varphi \, \mathsf{U} \, \neg\psi)$
  - ψ always holds, a requirement that is released as soon as φ holds
- Until U and release R are *dual*:

$$\varphi \, \mathsf{U} \, \psi \quad \equiv \quad \neg\varphi \, \mathsf{R} \, \neg\psi$$

$$\varphi \, \mathsf{R} \, \psi \quad \equiv \quad \neg(\neg\varphi \, \mathsf{U} \, \neg\psi)$$

- Until and release are *equally expressive*:
  - $\Box\psi \ \equiv \ \text{false} \, \mathsf{R} \, \psi$ and $\varphi \, \mathsf{U} \, \psi \ \equiv \ \neg\varphi \, \mathsf{R} \, \neg\psi$
- Release satisfies the *expansion law*: $\varphi \, \mathsf{R} \, \psi \equiv \psi \ \wedge \ (\varphi \ \vee \ \bigcirc(\varphi \, \mathsf{R} \, \psi))$

Semantics of release

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

iff (* definition of R *)

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

iff (* semantics of negation *)

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

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

$$\forall j \geqslant 0. \neg \left(\sigma[j..] \not\models \psi \wedge \forall i < j.\, \sigma[i..] \not\models \varphi \right)$$

iff (* de Morgan's law *)

$$\forall j \geqslant 0. \left(\neg(\sigma[j..] \not\models \psi) \vee \neg \forall i < j.\, \sigma[i..] \not\models \varphi \right)$$

iff (* semantics of negation *)

$$\forall j \geqslant 0. \left(\sigma[j..] \models \psi \vee \exists i < j.\, \sigma[i..] \models \varphi \right)$$

iff

$$\forall j \geqslant 0.\, \sigma[j..] \models \psi \quad \text{or} \quad \exists i \geqslant 0. \left(\sigma[i..] \models \varphi \right) \wedge \forall k \leqslant i.\, \sigma[k..] \models \psi \Big)$$

Positive normal form (revisited)

For $a \in AP$, LTL formulas in PNF are given by:

$$\varphi \ ::= \ \text{true} \ \Big| \ \text{false} \ \Big| \ a \ \Big| \ \neg a \ \Big| \ \varphi_1 \land \varphi_2 \ \Big| \ \varphi_1 \lor \varphi_2 \ \Big| \ \bigcirc \varphi \ \Big| \ \varphi_1 \, \mathsf{U} \, \varphi_2 \ \Big| \ \varphi_1 \, \mathsf{R} \, \varphi_2$$

PNF in linear size

For any LTL-formula φ there exists
an equivalent LTL-formula ψ in PNF with $|\psi| = \mathcal{O}(|\varphi|)$

Transformations:

$$
\begin{array}{lcl}
\neg\text{true} & \rightsquigarrow & \text{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi \wedge \psi) & \rightsquigarrow & \neg\varphi \vee \neg\psi \\
\neg(\varphi \vee \psi) & \rightsquigarrow & \neg\varphi \wedge \neg\psi \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc \neg\varphi \\
\neg(\varphi \,\mathsf{U}\, \psi) & \rightsquigarrow & \neg\varphi \,\mathsf{R}\, \neg\psi \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \\
\neg\Box\varphi & \rightsquigarrow & \Diamond\neg\varphi
\end{array}
$$