LTL formulas and models

▶ Examples from slide 75.
▶ Based on board-work during lecture 3.
▶ Example models, indicating whether the formula holds.

▶ Exercise: for failing models, give a counter-example path/trace.
▶ Reminder: LTL formulas are implicitly “for all paths”.

LTL formulas and models (1)

▶ “DeviceEnabled holds infinitely often along every path”
▶ $G(F\text{DeviceEnabled})$

LTL formulas and models (1)

▶ “DeviceEnabled holds infinitely often along every path”
▶ $G(F\text{DeviceEnabled})$
LTL formulas and models (1)

▶ “DeviceEnabled holds infinitely often along every path”
▶ $G(F \text{DeviceEnabled})$

LTL formulas and models (2)

▶ “Eventually the state becomes permanently Done”
▶ $F(G \text{Done})$

LTL formulas and models (2)

▶ “Eventually the state becomes permanently Done”
▶ $F(G \text{Done})$
LTL formulas and models (3)

- “Every Req is followed by an Ack”
- $G (Req \Rightarrow (F Ack))$

LTL formulas and models (3)

- “Every Req is followed by an Ack”
- $G (Req \Rightarrow (F Ack))$

LTL formulas and models (4)

- “Every Req is followed by an Ack”
- $G (Req \Rightarrow (F Ack))$

LTL formulas and models (4)

- “If Enabled infinitely often then Running infinitely often.”
- $G (F Enabled) \Rightarrow G (F Running)$
"If Enabled infinitely often then Running infinitely often."

$LTL$ formulas and models (4)

$G (F \text{Enabled}) \Rightarrow G (F \text{Running})$

Conrad Watt

Hoare Logic and Model Checking 14 / 25
The lift example is a little unwieldy, so here are some examples of $U$ in isolation instead.

$A U B$
LTL proofs (1)

- Prove \((M \models G \phi) \Rightarrow (M \models G (F \phi))\)
- Reminder:
  \[
  M \models \phi \iff \forall \pi. s \in S_0 \land \text{Path } R s \pi \Rightarrow \llbracket \phi \rrbracket_M(\pi)
  \]
- So sufficient to prove \([G \phi]_M(\pi) \Rightarrow [G (F \phi)]_M(\pi)\)
  (for arbitrary \(\pi\))

\[
\begin{align*}
\llbracket G \phi \rrbracket_M(\pi) & \equiv \forall i. \llbracket \phi \rrbracket_M(\pi \downarrow i) \\
& \equiv \forall i. \llbracket \phi \rrbracket_M(\pi \downarrow (i + 0)) \\
& \Rightarrow \forall i. \exists j. \llbracket \phi \rrbracket_M(\pi \downarrow (i + j)) \\
& \equiv \forall i. \exists j. \llbracket \phi \rrbracket_M(\pi \downarrow i \downarrow j) \\
& \equiv \forall i. \llbracket F \phi \rrbracket_M(\pi \downarrow i) \\
& \equiv \llbracket G (F \phi) \rrbracket_M(\pi) \quad \square
\end{align*}
\]

LTL proofs (2)

- Prove \((M \models G \phi) \equiv (M \models G (G \phi))\)
- Reminder:
  \[
  M \models \phi \iff \forall \pi. s \in S_0 \land \text{Path } R s \pi \Rightarrow \llbracket \phi \rrbracket_M(\pi)
  \]
- So sufficient to prove \([G \phi]_M(\pi) \equiv [G (G \phi)]_M(\pi)\)

\[
\begin{align*}
\llbracket G \phi \rrbracket_M(\pi) & \equiv \forall i. \llbracket \phi \rrbracket_M(\pi \downarrow i) \\
& \equiv \forall i. \llbracket \phi \rrbracket_M(\pi \downarrow (i + 0)) \\
& \equiv \forall i. \forall j. \llbracket \phi \rrbracket_M(\pi \downarrow (i + j)) \\
& \equiv \forall i. \forall j. \llbracket \phi \rrbracket_M(\pi \downarrow i \downarrow j) \\
& \equiv \forall i. \llbracket G \phi \rrbracket_M(\pi \downarrow i) \\
& \equiv \llbracket G (G \phi) \rrbracket_M(\pi) \quad \square
\end{align*}
\]
Prove $(M \models F (G \phi)) \Rightarrow (M \models G (F \phi))$

Reminder:

$M \models \phi \iff \forall \pi.s \in S_0 \land \text{Path } R s \pi \Rightarrow M(\pi) \models [\phi]$ 

So sufficient to prove $[F (G \phi)]_M(\pi) \Rightarrow [G (F \phi)]_M(\pi)$

$[F (G \phi)]_M(\pi)$

$\equiv \exists j. [G \phi]_M(\pi j)$

$\equiv \exists j. \forall i. [\phi]_M((\pi j) i)$

$\equiv \exists j. \forall i. [\phi]_M((\pi i) j)$

$[F (G \phi)]_M(\pi)$

$\equiv \exists i. [F \phi]_M(\pi i)$

$\equiv [G (F \phi)]_M(\pi)$

$\square$

Conrad Watt

Hoare Logic and Model Checking

25 / 25