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

- "DeviceEnabled holds infinitely often along every path"
- $G (F \text{DeviceEnabled})$
“Eventually the state becomes permanently Done”

\[ F (G \text{ Done}) \]
“Eventually the state becomes permanently Done”
$\mathcal{F}_{}$ $\mathcal{G}_{}$ Done
LTL formulas and models (2)

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

- “Every $\text{Req}$ is followed by an $\text{Ack}$”
- $G (\text{Req} \Rightarrow (F \text{ Ack}))$
LTL formulas and models (3)

- “Every Req is followed by an Ack”
- $G (\text{Req} \Rightarrow (F \text{Ack}))$
LTL formulas and models (3)

- “Every Req is followed by an Ack”
- $G (\text{Req} \Rightarrow (F \text{Ack}))$
LTL formulas and models (4)

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

$G (\neg F \text{ Enabled}) \rightarrow G (\neg F \text{ Running})$
LTL formulas and models (4)

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

\[ G (F \text{ Enabled}) \Rightarrow G (F \text{ Running}) \]
LTL formulas and models (4)

- “If Enabled infinitely often then Running infinitely often.”
- $G (F \text{ Enabled}) \Rightarrow G (F \text{ Running})$
The lift example is a little unwieldy, so here are some examples of $U$ in isolation instead.

$A U B$
LTL formulas and models (5)

A \cup B
LTL formulas and models (5)

\[ \mathbb{A} \cup \mathbb{B} \]
LTL formulas and models (5)
LTL formulas and models (5)

\[ A \cup U \emptyset \]

\[ \text{START} \rightarrow \text{START} \]

\[ \text{B} \]

\[ \text{X} \]
LTL proofs

- Example proofs of LTL implications and equivalences.
- Based on board-work during lecture 3.
LTL proofs (1)

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

\[
\begin{align*}
[G \phi]_M(\pi) &\equiv \forall i. [\phi]_M(\pi \downarrow i) \\
&\equiv \forall i. [\phi]_M(\pi \downarrow (i + 0)) \\
&\Rightarrow \forall i. \exists j. [\phi]_M(\pi \downarrow (i + j)) \\
&\equiv \forall i. \exists j. [\phi]_M((\pi \downarrow i) \downarrow j) \\
&\equiv \forall i. [F \phi]_M(\pi \downarrow i) \\
&\equiv [G (F \phi)]_M(\pi) \quad \Box
\end{align*}
\]
LTL proofs (2)

▶ Prove \((M \models G \phi) \equiv (M \models G (G \phi))\)

▶ Reminder:
\[
M \models \phi \iff \forall \pi \ s. \ s \in S_0 \land \text{Path } R s \pi \Rightarrow \llbracket \phi \rrbracket_M(\pi)
\]

▶ So sufficient to prove \(\llbracket G \phi \rrbracket_M(\pi) \equiv \llbracket G (G \phi) \rrbracket_M(\pi)\)

\[
\llbracket G \phi \rrbracket_M(\pi)
\equiv \forall i. \llbracket \phi \rrbracket_M(\pi \downarrow i)
\equiv \forall i. \forall j. \llbracket \phi \rrbracket_M(\pi \downarrow (i + j))
\equiv \forall i. \forall j. \llbracket \phi \rrbracket_M((\pi \downarrow i) \downarrow j)
\equiv \forall i. \llbracket G \phi \rrbracket_M(\pi \downarrow i)
\equiv \llbracket G (G \phi) \rrbracket_M(\pi)
\]

\[
\square
\]

Conrad Watt
Hoare Logic and Model Checking 24 / 25
LTL proofs (3)

- Prove $(M \models F (G \phi)) \Rightarrow (M \models G (F \phi))$
- Reminder:

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

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

$$[[F (G \phi)]_M(\pi)$$
$$\equiv \exists j. \ [[G \phi]_M(\pi \downarrow j)$$
$$\equiv \exists j. \ \forall i. \ [[\phi]_M((\pi \downarrow j) \downarrow i)$$
$$\equiv \exists j. \ \forall i. \ [[\phi]_M((\pi \downarrow i) \downarrow j)$$
$$\Rightarrow \ \forall i. \ \exists j. \ [[\phi]_M((\pi \downarrow i) \downarrow j)$$
$$\equiv \ \forall i. \ [[F \phi]_M(\pi \downarrow i)$$
$$\equiv [[G (F \phi)]_M(\pi)$$