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".



3 / 25 Conrad Watt

"DeviceEnabled holds infinitely often along every path" ►

UNIVERSITY OF CAMBRIDGE

Hoare Logic and Model Checking

Model Checking Lecture 3 Supplement

Conrad Watt

Computer Laboratory, University of Cambridge, UK http://www.cl.cam.ac.uk/~caw77 CST Part II - 2018/19

G (F DeviceEnabled)

- "DeviceEnabled holds infinitely often along every path"
- ► G (F DeviceEnabled)



Hoare Logic and Model Checking





Hoare Logic and Model Checking

LTL formulas and models (1)

LTL formulas and models (2)

- "DeviceEnabled holds infinitely often along every path"
- ► G (F DeviceEnabled)



- "Eventually the state becomes permantently Done"
- ► F (G Done)



- 5/25 Contrad Watt Heare Logic and Model Checking
 LTL formulas and models (2)
 - "Eventually the state becomes permantently Done"
 - ► F (G Done)



Conrad Watt

Hoare Logic and Model Checking

LTL formulas and models (2)

- "Eventually the state becomes permantently Done"
- ► F (G Done)





6/25

LTL formulas and models (3)

LTL formulas and models (3)

- "Every Reg is followed by an Ack" $\blacktriangleright \mathbf{G} (\mathbf{Req} \Rightarrow (\mathbf{F} \mathbf{Ack}))$
 - START

- "Every Reg is followed by an Ack"
- ▶ $G(\text{Reg} \Rightarrow (F \text{Ack}))$





- Hoare Logic and Model Checking 9/25 Conrad Watt Hoare Logic and Model Checking 10/25 LTL formulas and models (3) LTL formulas and models (4)
 - "Every Reg is followed by an Ack"
 - G (Req \Rightarrow (F Ack))





- "If Enabled infinitely often then Running infinitely often."
- ▶ $G(FEnabled) \Rightarrow G(FRunning)$



Conrad Watt

Conrad Watt

LTL formulas and models (4)

► G (F Enabled) ⇒ G (F Running)

LTL formulas and models (4)

- "If Enabled infinitely often then Running infinitely often."
- $\blacktriangleright \ \textbf{G} \ (\textbf{F} \ \textbf{Enabled}) \Rightarrow \textbf{G} \ (\textbf{F} \ \textbf{Running})$



"If Enabled infinitely often then Running infinitely often."

"If Enabled infinitely often then Running infinitely often."

 $\blacktriangleright \ G \ (F \ \texttt{Enabled}) \Rightarrow G \ (F \ \texttt{Running})$



- "If Enabled infinitely often then Running infinitely often."
- ► G (F Enabled) ⇒ G (F Running)



LTL formulas and models (5)

LTL formulas and models (5)

The lift example is a little unwieldy, so here are some examples of U in isolation instead.

► A U B



🕨 A U B





► A U B

υв





► A U B



LTL formulas and models (5)

LTL proofs

► A U B



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



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

```
\begin{bmatrix} \mathbf{G} \phi \end{bmatrix}_{M}(\pi) \\ \equiv \forall i. \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi j l) \\ \equiv \forall i. \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi j l) \\ \Rightarrow \forall i. \exists j. \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi j (i + 0)) \\ \Rightarrow \forall i. \exists j. \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi j (i + j)) \\ \equiv \forall i. \begin{bmatrix} F \phi \end{bmatrix}_{M}(\pi j l) \\ \equiv \forall i. \begin{bmatrix} F \phi \end{bmatrix}_{M}(\pi j l) \\ \equiv \begin{bmatrix} \mathbf{G} \begin{bmatrix} F \phi \end{bmatrix}_{M}(\pi j) \\ \end{bmatrix}
```

▶ Prove $(M \models \mathbf{G} \phi) \equiv (M \models \mathbf{G} (\mathbf{G} \phi))$

► Reminder: $M \models \phi \Leftrightarrow \forall \pi \ s. \ s \in S_0 \land \text{Path } R \ s \ \pi \Rightarrow \llbracket \phi \rrbracket_M(\pi)$

So sufficient to prove $[\mathbf{G} \phi]_M(\pi) \equiv [\mathbf{G} (\mathbf{G} \phi)]_M(\pi)$

 $\begin{bmatrix} \mathbf{G} & \phi \end{bmatrix}_{M}(\pi) \\ \equiv \forall i. & \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi \downarrow i) \\ \equiv \forall i. & \forall j. & \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi \downarrow (i + j)) \\ \equiv \forall i. & \forall j. & \begin{bmatrix} \phi \end{bmatrix}_{M}(\pi \downarrow i) \downarrow j) \\ \equiv \forall i. & \begin{bmatrix} \mathbf{G} & \phi \end{bmatrix}_{M}(\pi \downarrow i) \\ \equiv \begin{bmatrix} \mathbf{G} & (\mathbf{G} & \phi) \end{bmatrix}_{M}(\pi) \square$

LTL proofs (3)

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

 $\begin{bmatrix} \mathbf{F} (\mathbf{G} \phi) \end{bmatrix}_{M} (\pi) \\ \equiv \exists j. \begin{bmatrix} \mathbf{G} \phi \end{bmatrix}_{M} (\pi \mathbf{i} j) \\ \equiv \exists j. \forall i. \begin{bmatrix} \phi \phi \end{bmatrix}_{M} ((\pi \mathbf{i} j) \mathbf{j} i) \\ \equiv \exists j. \forall i. \begin{bmatrix} \phi \phi \end{bmatrix}_{M} ((\pi \mathbf{i} i) \mathbf{j} j) \\ \Rightarrow \forall i. \exists j. \begin{bmatrix} \phi \phi \end{bmatrix}_{M} ((\pi \mathbf{i} i) \mathbf{j} j) \\ \equiv \forall j. \begin{bmatrix} \mathbf{F} \phi \end{bmatrix}_{M} (\pi \mathbf{i} j) \\ \equiv \begin{bmatrix} \mathbf{G} (\mathbf{F} \phi) \end{bmatrix}_{M} (\pi) \Box$

Conrad Watt

Hoare Logic and Model Checking

25/25