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

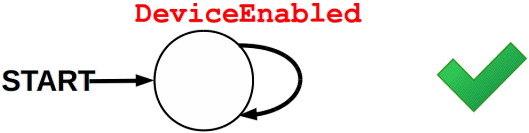
LTL formulas and models

- 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”.

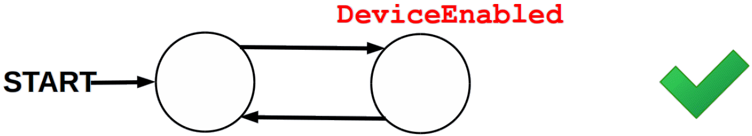
LTL formulas and models (1)

- “**`DeviceEnabled`** holds infinitely often along every path”
- **G (F `DeviceEnabled`)**



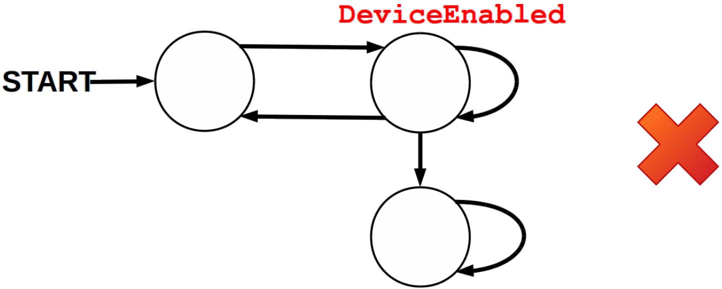
LTL formulas and models (1)

- “DeviceEnabled holds infinitely often along every path”
- G (F DeviceEnabled)



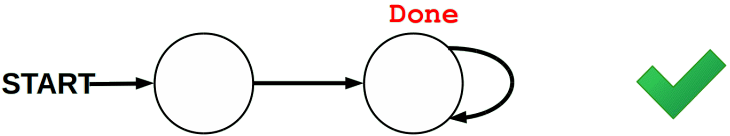
LTL formulas and models (1)

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



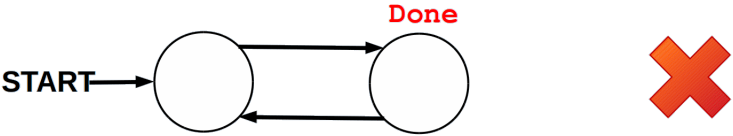
LTL formulas and models (2)

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



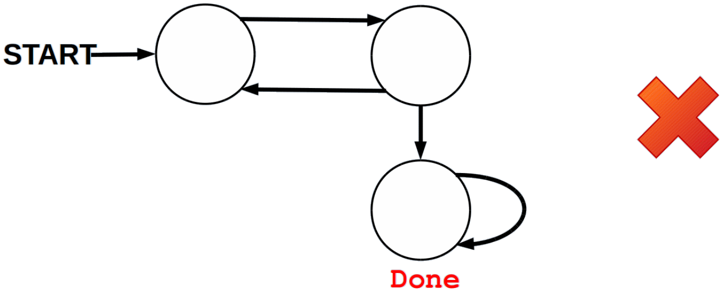
LTL formulas and models (2)

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



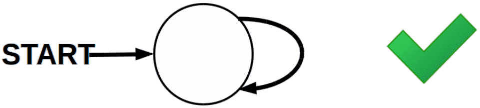
LTL formulas and models (2)

- “Eventually the state becomes permantently **Done**”
- **F (G Done)**



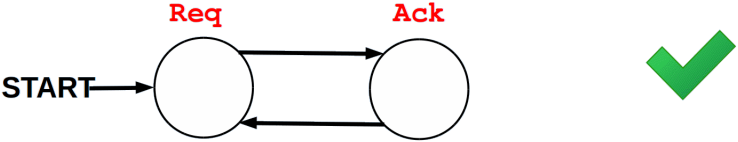
LTL formulas and models (3)

- "Every **Req** is followed by an **Ack**"
- $\mathbf{G}\ (\mathtt{Req} \Rightarrow (\mathbf{F}\ \mathtt{Ack}))$



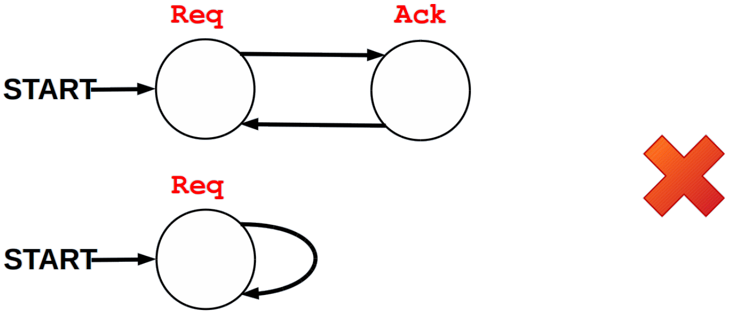
LTL formulas and models (3)

- "Every **Req** is followed by an **Ack**"
- $\mathbf{G}\ (\mathtt{Req} \Rightarrow (\mathbf{F}\ \mathtt{Ack}))$



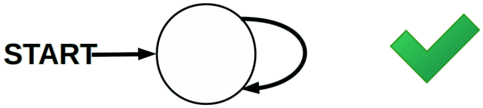
LTL formulas and models (3)

- “Every **Req** is followed by an **Ack**”
- $\mathbf{G}\ (\mathtt{Req} \Rightarrow (\mathbf{F}\ \mathtt{Ack}))$



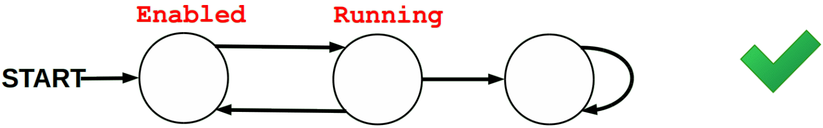
LTL formulas and models (4)

- "If `Enabled` infinitely often then `Running` infinitely often."
- $\mathbf{G}\ (\mathbf{F}\ \texttt{Enabled}) \Rightarrow \mathbf{G}\ (\mathbf{F}\ \texttt{Running})$



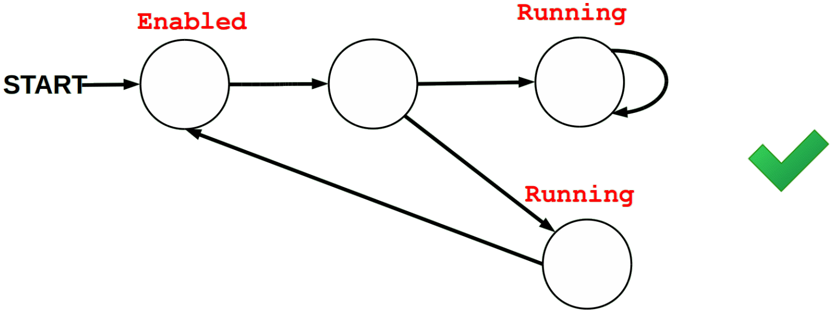
LTL formulas and models (4)

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



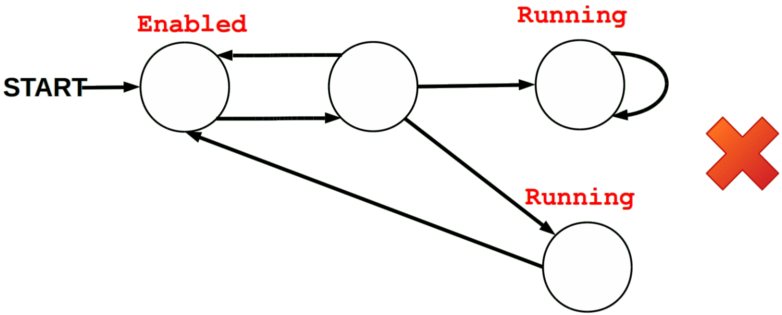
LTL formulas and models (4)

- "If `Enabled` infinitely often then `Running` infinitely often."
- $\mathbf{G}\ (\mathbf{F}\ \texttt{Enabled}) \Rightarrow \mathbf{G}\ (\mathbf{F}\ \texttt{Running})$



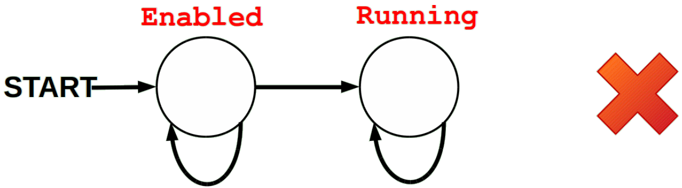
LTL formulas and models (4)

- "If `Enabled` infinitely often then `Running` infinitely often."
- $\mathbf{G}\ (\mathbf{F}\ \texttt{Enabled}) \Rightarrow \mathbf{G}\ (\mathbf{F}\ \texttt{Running})$



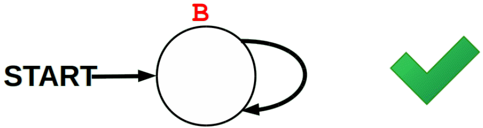
LTL formulas and models (4)

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



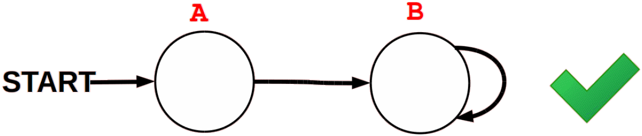
LTL formulas and models (5)

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



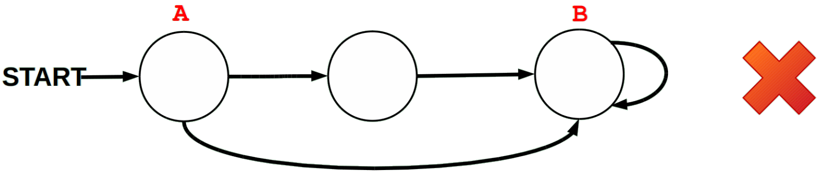
LTL formulas and models (5)

- A U B



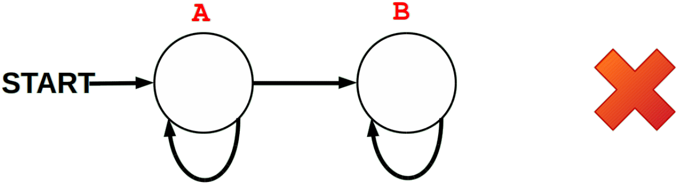
LTL formulas and models (5)

- **A U B**



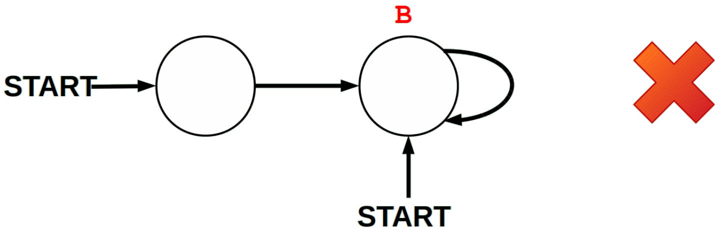
LTL formulas and models (5)

- **A U B**



LTL formulas and models (5)

- **A U B**



LTL proofs

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

LTL proofs (1)

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

$$
\begin{aligned}
& [\![\mathbf{G}\ \phi]\!]_M(\pi) \\
\equiv\ & \forall i.\ [\![\phi]\!]_M(\pi{\downarrow}i) \\
\equiv\ & \forall i.\ [\![\phi]\!]_M(\pi{\downarrow}(i+0)) \\
\Rightarrow\ & \forall i.\ \exists j.\ [\![\phi]\!]_M(\pi{\downarrow}(i+j)) \\
\equiv\ & \forall i.\ \exists j.\ [\![\phi]\!]_M((\pi{\downarrow}i){\downarrow}j) \\
\equiv\ & \forall i.\ [\![\mathbf{F}\ \phi]\!]_M(\pi{\downarrow}i) \\
\equiv\ & [\![\mathbf{G}\ (\mathbf{F}\ \phi)]\!]_M(\pi) \quad \square
\end{aligned}
$$

LTL proofs (2)

- Prove $(M \models \mathbf{G}\ \phi) \equiv (M \models \mathbf{G}\ (\mathbf{G}\ \phi))$
- Reminder:

$$\boxed{M \models \phi \;\Leftrightarrow\; \forall \pi\ s.\ s \in S_0 \wedge \text{Path}\ R\ s\ \pi \Rightarrow [\![\phi]\!]_M(\pi)}$$

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

$$
\begin{aligned}
& [\![\mathbf{G}\ \phi]\!]_M(\pi) \\
& \equiv \forall i.\ [\![\phi]\!]_M(\pi{\downarrow}i) \\
& \equiv \forall i.\ \forall j.\ [\![\phi]\!]_M(\pi{\downarrow}(i + j)) \\
& \equiv \forall i.\ \forall j.\ [\![\phi]\!]_M((\pi{\downarrow}i){\downarrow}j) \\
& \equiv \forall i.\ [\![\mathbf{G}\ \phi]\!]_M(\pi{\downarrow}i) \\
& \equiv [\![\mathbf{G}\ (\mathbf{G}\ \phi)]\!]_M(\pi) \quad \square
\end{aligned}
$$

LTL proofs (3)

- Prove $(M \models \mathbf{F}\ (\mathbf{G}\ \phi)) \Rightarrow (M \models \mathbf{G}\ (\mathbf{F}\ \phi))$
- Reminder:
  $\boxed{M \models \phi \;\Leftrightarrow\; \forall \pi\ s.\ s \in S_0 \wedge \text{Path } R\ s\ \pi \Rightarrow [\![\phi]\!]_M(\pi)}$
- So sufficient to prove $[\![\mathbf{F}\ (\mathbf{G}\ \phi)]\!]_M(\pi) \Rightarrow [\![\mathbf{G}\ (\mathbf{F}\ \phi)]\!]_M(\pi)$

$$
\begin{aligned}
& [\![\mathbf{F}\ (\mathbf{G}\ \phi)]\!]_M(\pi) \\
\equiv\ & \exists j.\ [\![\mathbf{G}\ \phi]\!]_M(\pi{\downarrow}j) \\
\equiv\ & \exists j.\ \forall i.\ [\![\phi]\!]_M((\pi{\downarrow}j){\downarrow}i) \\
\equiv\ & \exists j.\ \forall i.\ [\![\phi]\!]_M((\pi{\downarrow}i){\downarrow}j) \\
\Rightarrow\ & \forall i.\ \exists j.\ [\![\phi]\!]_M((\pi{\downarrow}i){\downarrow}j) \\
\equiv\ & \forall i.\ [\![\mathbf{F}\ \phi]\!]_M(\pi{\downarrow}i) \\
\equiv\ & [\![\mathbf{G}\ (\mathbf{F}\ \phi)]\!]_M(\pi) \qquad \square
\end{aligned}
$$