Hoare Logic and Model Checking
Model Checking Lecture 4 Supplement

Conrad Watt

Computer Laboratory, University of Cambridge, UK
http://www.cl.cam.ac.uk/~caw77

CST Part II – 2018/19
CTL formulas and models

- Examples from slide 91.
- Based on board-work during lecture 4.
- Example models, indicating whether the formula holds.
- Exercise: for failing models, give a counter-example path/trace.
CTL formulas and models (1)

▶ “It is possible to get to a state where \textit{Started} holds but \textit{Ready} does not hold.”
▶ $\text{EF} (\text{Started} \land \neg \text{Ready})$

▶ Exercise: compare to the \textbf{LTL} formula
$\text{F} (\text{Started} \land \neg \text{Ready})$
CTL formulas and models (1)

▶ “It is possible to get to a state where \textit{Started} holds but \textit{Ready} does not hold.”
▶ $\text{EF} (\text{Started} \land \neg \text{Ready})$

Exercise: compare to the \textit{LTL} formula

$\text{F} (\text{Started} \land \neg \text{Ready})$
CTL formulas and models (2)

▶ “If a request $\text{Req}$ occurs, then it will be eventually acknowledged by $\text{Ack}$.”

▶ $\mathsf{AG} (\text{Req} \implies \mathsf{AF} \text{Ack})$

Exercise: compare to the $\mathsf{LTL}$ formula $\mathsf{G} (\text{Req} \implies \mathsf{F} \text{Ack})$
CTL formulas and models (2)

▶ “If a request $\text{Req}$ occurs, then it will be eventually acknowledged by $\text{Ack}$.”

▶ $\text{AG} (\text{Req} \implies \text{AF Ack})$

▶ Exercise: compare to the $\text{LTL}$ formula $\text{G} (\text{Req} \implies \text{F Ack})$
CTL formulas and models (2)

- “If a request $\text{Req}$ occurs, then it will be eventually acknowledged by $\text{Ack}$.”
- $\text{AG} (\text{Req} \Rightarrow \text{AF Ack})$

Exercise: compare to the LTL formula $\text{G} (\text{Req} \Rightarrow \text{F Ack})$
 CTL formulas and models (3)

- “DeviceEnabled is always true somewhere along every path starting anywhere: i.e. DeviceEnabled holds infinitely often along every path.”
- \(\text{AG (AF DeviceEnabled)}\)

- Exercise: compare to the LTL formula \(\text{G (F DeviceEnabled)}\)
CTL formulas and models (3)

- “DeviceEnabled is always true somewhere along every path starting anywhere: i.e. DeviceEnabled holds infinitely often along every path.”
- $\text{AG} (\text{AF DeviceEnabled})$

Exercise: compare to the LTL formula $G (F \text{DeviceEnabled})$
“DeviceEnabled is always true somewhere along every path starting anywhere: i.e. DeviceEnabled holds infinitely often along every path.”

AG (AF DeviceEnabled)

Exercise: compare to the LTL formula G (F DeviceEnabled)
CTL formulas and models (4)

- From any state it is possible to get to a state for which “Restart holds.”
- \(\text{AG} (\text{EF} \text{Restart})\)

Exercise: compare to the LTL formula \(\text{G} (\text{F} \text{Restart})\)
From any state it is possible to get to a state for which “\textit{Restart} holds.”

\[ AG (EF \textit{Restart}) \]

Exercise: compare to the \textbf{LTL} formula
\[ G (F \textit{Restart}) \]
Misc CTL exercises (1)

- $\text{AG (Req } \Rightarrow \text{ AX(A[\neg \text{Req U Ack}]})$

- Is the formula $\text{AG (Req } \Rightarrow \text{ A[\neg \text{Req U Ack}]})$ equivalent?

- Easy to construct a counter-example: the second formula requires that $\text{Ack}$ is true immediately when $\text{Req}$ is true.
Misc CTL exercises (2)

▶ AG (Req ⇒ (¬Ack ⇒ AX(A[Req U Ack])))

▶ Can we simplify the formula?

AG (Req ⇒ (¬Ack ⇒ AX(A[Req U Ack])))
≡ AG ((Req ∧ ¬Ack) ⇒ AX(A[Req U Ack]))
≡ AG ((Req ∧ ¬Ack) ⇒ (A[Req U Ack]))

▶ Exercise: are these equivalence steps correct?

▶ Extended: do we have to assume that our model is left-total?