CTL Model-Checking

Deepak D'Souza

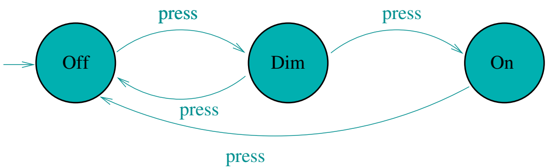
Department of Computer Science and Automation
Indian Institute of Science, Bangalore.

9 January 2018

Overview and Motivation

- Consider systems as Transition Systems
- Can specify branching properties of the system.
- Can check these properties algorithmically by “labelling” the states of the model.

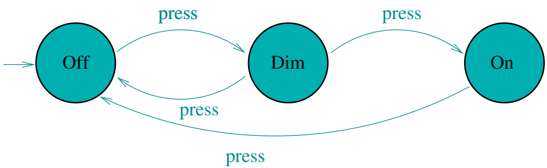
Light Switch Model



There is a state from which both “Off” and “On” state are possible next states.
In CTL:

$$EF(EX\ \mathit{Off} \wedge EX\ \mathit{On})$$

Light Switch Model



There is a state from which both “Off” and “On” state are possible next states.
In CTL:

$$EF(EX\ Off \land EX\ On)$$

Does the model satisfy the property

$$AG(Off \implies AF\ On)?$$

Computational Tree Logic (CTL)

- State formulas f (evaluated at a state in the TS):

$$f ::= p \mid \neg f \mid f \vee g \mid f \wedge g \mid E\, g \mid A\, g$$

  where p is a proposition, and g is a path formula.
- Path formulas g (evaluated along a path in the TS):

$$g ::= X\, f \mid F\, f \mid G\, f \mid f\, U\, f'$$

Examples:

- $AG(On \implies EX\, Off)$ is a CTL formula
- $AG(G\, F\, On)$ is *not* a CTL formula

Exercise

Give a transition system M with states s and s' in M, where the following CTL formulas are satisfied at s but not at s':

1. $\mathrm{EFAX}p$

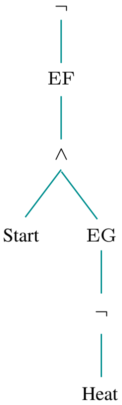
Exercise

Give a transition system M with states s and s' in M, where the following CTL formulas are satisfied at s but not at s':

1. $\mathrm{EFAX}p$
2. $\mathrm{AFE}(p \mathrm{~U~} q)$

CTL model-checking algorithm

- Label each state with the sub-formulas of given formula f (bottom-up)
- States are labelled f are the ones that satisfy the formula.



Example: $\neg EF(Start \wedge EG \neg Heat)$

CTL model-checking algo

- All formulas can be reduced to modalities EX, EG, EU.
- To check $f = EXp$, label all states s with f iff from s there is a transition to a state s' labelled p.
- To check $f = EGp$, label all states s with f iff from s there is a path to a non-trivial strongly connected component, in the subgraph of states labelled p.
- To check $f = E(pUq)$, label all states s with f iff from s there is a path of p-labelled states to a state labelled q.

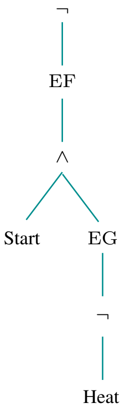
CTL model-checking algo by example: Microwave model

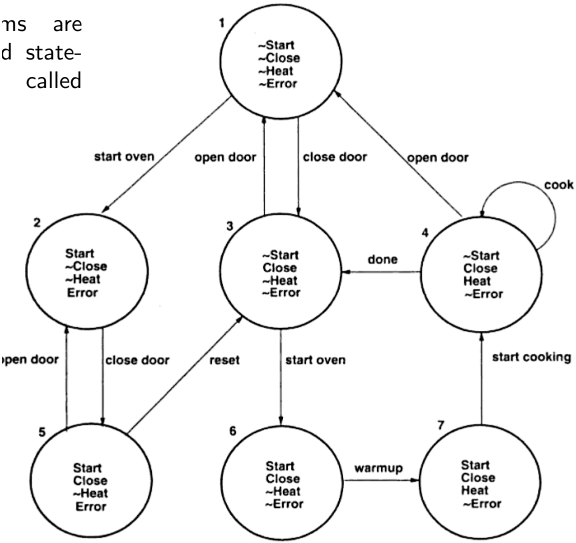
$AG(Start \implies AFHeat)$

Equivalently:

$\neg EF(Start \wedge EG \neg Heat)$

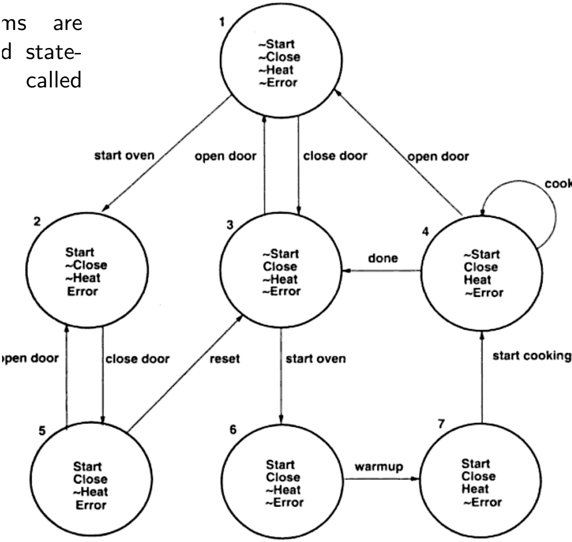
ms are
d state-
called





Exercise

ms are
d state-
called



Does the microwave model satisfy:
$AG(Error \implies AF\neg Error)$?

Run the CTL model-checking algo to find out.

Resources

- Clarke, Grumberg and Peled: Model Checking, MIT Press, 1999.
- Tools: Sal (SRI), NuSMV