COL750: Foundations of Automatic Verification (Jan-May 2023)

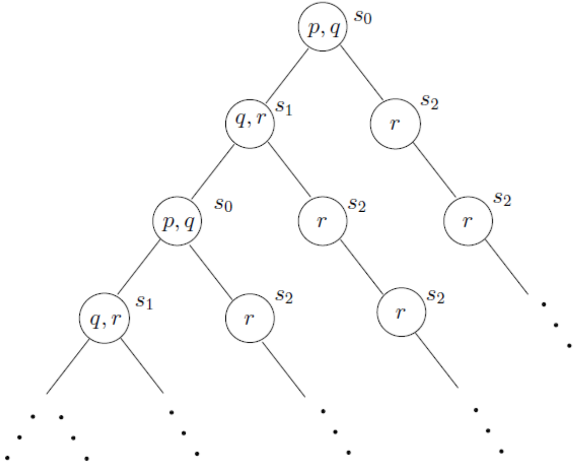
Lectures 05 & 06 (CTL Model Checking)

Kumar Madhukar

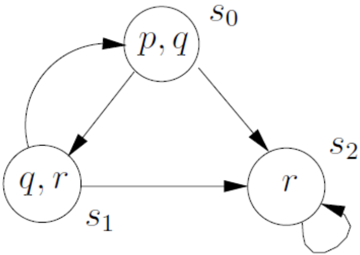
madhukar@cse.iitd.ac.in

Jan 19th and 23rd

Example



Example



Example specifications

- it is possible to get to a state where started holds, but ready does not hold

Example specifications

- it is possible to get to a state where started holds, but ready does not hold
- it is impossible ...

Example specifications

- for any state, if a request occurs, then it will eventually be granted

Example specifications

- a certain process is enabled infinitely often on every computational path

Example specifications

- on all paths, a certain process will eventually become (permanently) deadlocked

Example specifications

- if a process is enabled infinitely often, then it runs infinitely often

Example specifications

- from any state, it is possible to get to a restart state

Example specifications

- an upward travelling lift at the second floor does not change its direction if the fifth floor button is pressed

Example specifications

- the lift *can* remain idle on the third floor with its doors closed

Example specifications

- Non-blocking – a process can always request to enter its critical section

Example specifications

- No strict sequencing – processes need not enter their critical section in strict sequence

LTL and CTL

- LTL: what atomic proposition (or their boolean combinations) are true (or not true) in a state
- LTL: what is true about all paths starting from here
- CTL: we look at the entire tree of computation paths

Benefits of both

- state formulas
- path formulas

Restrictions in CTL

- boolean combination of path formulas
- nesting of path modalities

Boolean combination of path formulas

- only an apparent restriction
- can find equivalent formulas in CTL
- e.g. $\mathtt{E(F\ p} \wedge \mathtt{F\ q)}$

Back to example specifications

- on all paths, a certain process will eventually become (permanently) deadlocked

AF AG p $\neq$ F G p

- in fact, AF AG p is strictly stronger than FG p
- it is possible that FG p is true but AF AG p is not true in a model
- whenever AF AG p is true, FG p is also true
- so, in CTL, we have specified a stronger property than what is needed to capture the requirement

Comparing expressive powers

- in LTL as well as CTL: AGp in CTL is same as Gp in LTL
- in CTL but not in LTL: AG EF p in CTL does not have a corresponding formula in LTL (for proof, refer to Huth and Ryan, Sect. 3.5)
- in LTL but not in CTL: FG p (we saw earlier)
- neither LTL/CTL, but in CTL*: E[GF p] (there exists a path with infinitely many p's)

CTL Model Checking

- Refer to pages 222-224 (of Sect. 3.6.1) of the book by Huth and Ryan

- for examples, refer to slides by Prof. B. Srivathsan (from CMI): `https://www.cmi.ac.in/~sri/Courses/NPTEL/ModelChecking/Slides/Unit10-Module2.pdf`

Thank you!