

Lecture 1 - January 10

Syllabus & Introduction

***Safety-Critical Systems
Verification vs. Validation
Theorem Proving vs. Model Checking
TLA+***

theorem proving (3342)

model checking (4315)

formal methods

manual, semi-automated

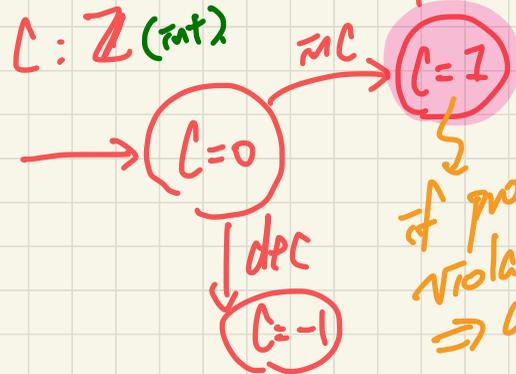
stop by step via relevant inference rules by hands

human intervention for the prover to complete

- no state ex. concern
- challenge: discharge PPs.

automated based on your specification, a graph is generated.

BUT suffers from state explosion problem



if property is gen-violated => a witness ex (counter trace)

New Language design

✓
ANTLR4

4302 F22

TCA+

- - - - ->

model checking.

Logic covered

ECS 3342 :

untimed.
proposition / predicates

ECS 4315 :

temporal logic

relative
notion of
time

- eventually P holds
- infinitely often P holds

LTL - linear temporal logic
CTL - computation tree logic