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

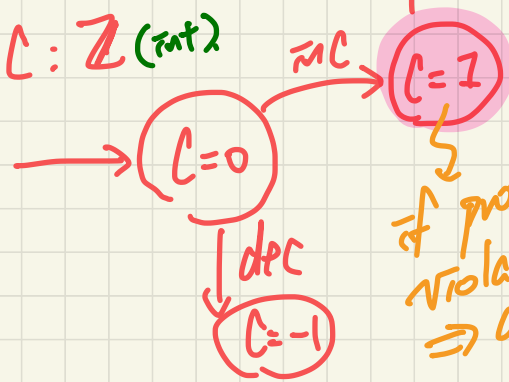
manual, semi-automated

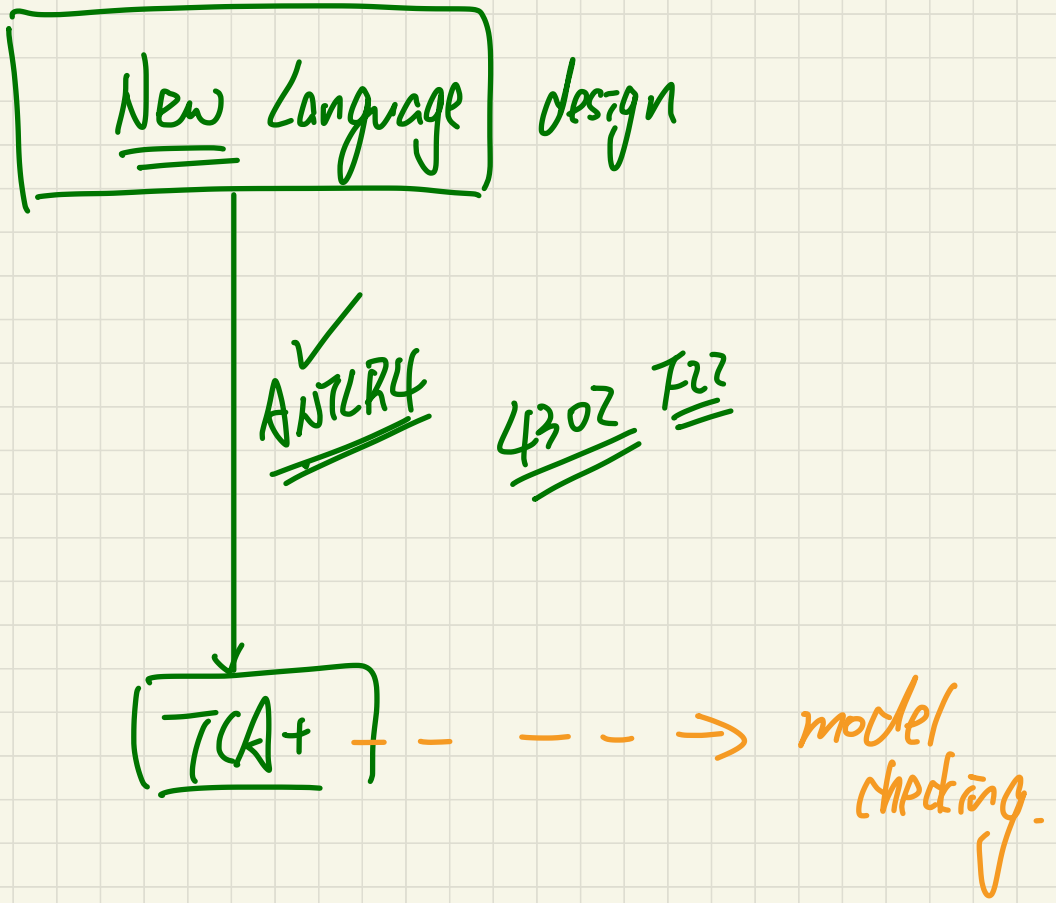
- step by step via relevant inference rules by hands
- human intervention for the prover to complete
- no state ex. concern
- challenge: discharge POs.

automated

based on your specification, a graph is generated.

BUT suffers from state explosion problem




New Language design
ANTLR4
4302 Fzz
TCA+
model checking.

Logic covered

EECS 3342 :

EECS 4315 :