Lecture 1 - Sep. 5

Syllabus & Introduction

Formal Methods:
Theorem Proving vs. Model Checking

Course Learning Outcomes (CLOs)

CLO1 Document requirements organizing them into appropriate categories such as environmental constraints versus functional properties (safety and progress).

CLO2 Construct high level, abstract mathematical models of a system (consisting of both the system and its environment) amenable to formal reasoning.

CLO3 Apply set theory and predicate logic to express functional and safety properties from the requirements as events, guards, system variants and invariants of a state-event model.

CLO4 Use models to reason about and predict their safety and progress properties.

CLO5 Plan and construct a sequence of refinements from abstract high-level specifications to implemented code.

CLO6 Prove that a concrete system refines an abstract model.

CLO7 Apply the method to a variety of systems such as sequential, concurrent and embedded systems.

CLO8 Use practical tools for constructing and reasoning about the models.

CLO9 Use Hoare Logic and Dijkstra weakest precondition calculus to derive correct designs.

mathematical

Formal Methods

discrete math

(∵ computer system is discrete (0,1))

$x \in \{1..10\}$

$y \in \{1..5\}$

- 3342
  - theorem proving
    - manual (interactions with prover)
    - deductions, constants, variables, axioms, invariants ⇒ properties?
- 4315 Mission-Critical system
  - model checking
    - model + properties? → model checker
      - yes → proved
      - no → not proved (counter example)
    - state explosion
    - (tool does not halt)
    - system is too large for the tool to conclude