UNIT V – Verifying Temporal Properties

Introduction to Temporal Property Verification

Formal Methods | MNNIT

-Dr. Varsha Singh

Lecture Objectives

- Understand what temporal properties are
- Differentiate between safety and liveness properties
- Appreciate the role of temporal logic in system verification
- Introduce how properties are verified using model checking

What Are Temporal Properties?

- Temporal properties express how systems evolve over time
- Go beyond static input/output correctness
- Fundamental to reactive systems, where behavior is ongoing

Types of Temporal Properties

- **Safety:** 'Something bad never happens' (e.g., system never deadlocks)
- **Liveness:** 'Something good eventually happens' (e.g., request is eventually granted)

Why Are Temporal Properties Important?

- Ensure correctness over time
- Catch issues that unit tests may miss
- Help verify concurrency, fairness, and responsiveness

Common Examples of Temporal Properties

- Deadlock freedom (Safety)
- Eventual resource release (Liveness)
- Mutual exclusion (Safety)
- Guaranteed access (Liveness)

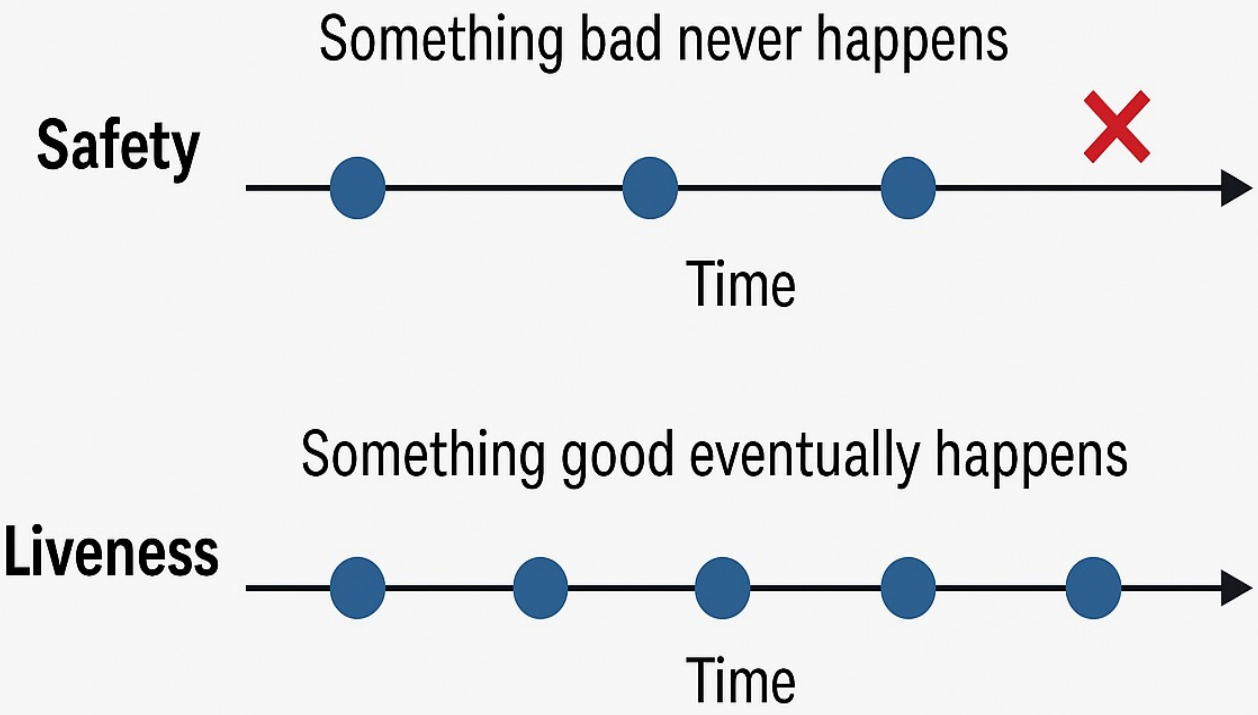
Specification Using Temporal Logic

- Formal logics used: LTL (Linear Temporal Logic), CTL (Computation Tree Logic)
- Formal syntax & semantics allow automated checking

Example – Liveness in an Elevator System

- 'The elevator eventually serves every floor'
- Liveness property
- In LTL: G(request → F(serve))

Safety vs. Liveness – A Visual Analogy

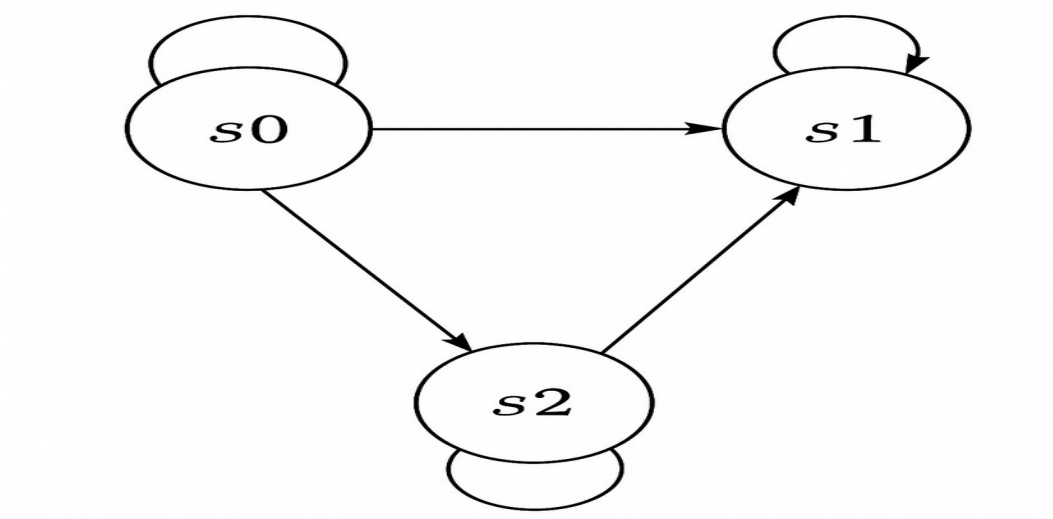


Role of Model Checking

- Automated technique to verify temporal properties
- Explores system states
- Compares against formal specification
- Provides counterexamples if the property fails

Kripke Structure

- Mathematical model used in model checking
- Components: States, Transitions, Labeling function (atomic propositions)



Recap and Transition

- Temporal properties capture time-dependent behavior
- Two key types: Safety and Liveness
- Formal logics help specify them
- Next: How to verify them using CTL model checking

Questions

- What would be a liveness property for a login system?
- Can safety and liveness overlap?
- Why can't we use just unit testing?

References

- Baier & Katoen, Principles of Model Checking
- Clarke, Grumberg, and Peled, Model Checking