Lecture 22: Analysis

Kenneth M. Anderson

Foundations of Software Engineering

CSCI 5828 - Spring Semester, 1999

Today's Lecture

- Examine Static and Dynamic Analysis
  - On Petri Nets

Analysis of Specifications

- Design is a Human Activity

  Can be wrong; can change
- Verification and Validation
- V&V are "W.R.T." Activities
- A Confidence Game

  V&V can only be used to raise confidence in the quality of a specification

Approaches to Analysis

- Dynamic Analysis
  - Executes specification text to reveal properties
  - Requires executable specifications
  - Example: testing
- Static Analysis
  - Examines specification text to reveal properties
  - Useful in the absence of execution semantics, but also where execution would be impractical
  - Example: proof of correctness

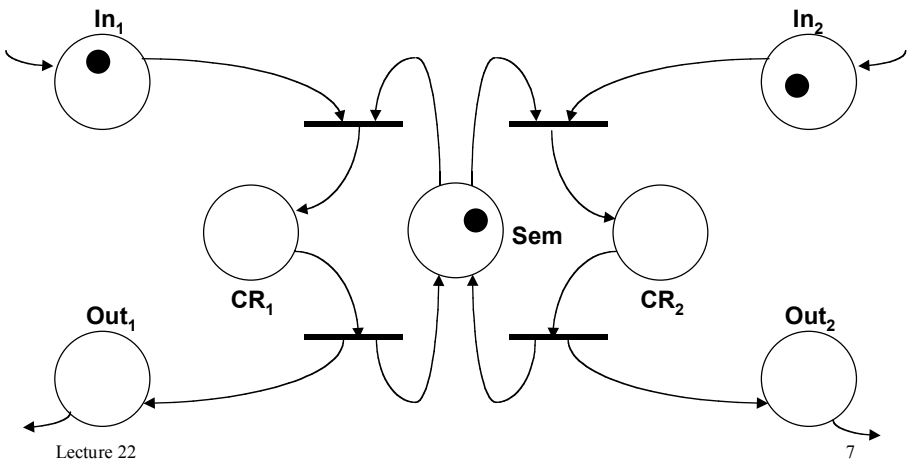
Dynamic Analysis

- An Experimentation Activity
- Goal: Demonstrate (In)correct Behavior
- An Experiment Characterizes a Single Behavior
- Applied to the Artifact Itself
- Can Miss Critical Behaviors
- In General, Impossible to Demonstrate Absence of Error

Petri Net Dynamic Analysis

- Reachability Graph
  - The *reachability graph* of a Petri net is a graph representation of its possible firing sequences
- Analysis Cast as Search for Node in Reachability Graph
  - Found, means behavior possible, not found means behavior impossible

Two-process Semaphore



Petri Net Dynamic Analysis

- Example: Two-process Semaphore

  Is it possible for both processes to be in their critical regions at the same time in the same marking? That is, is the following a valid marking?

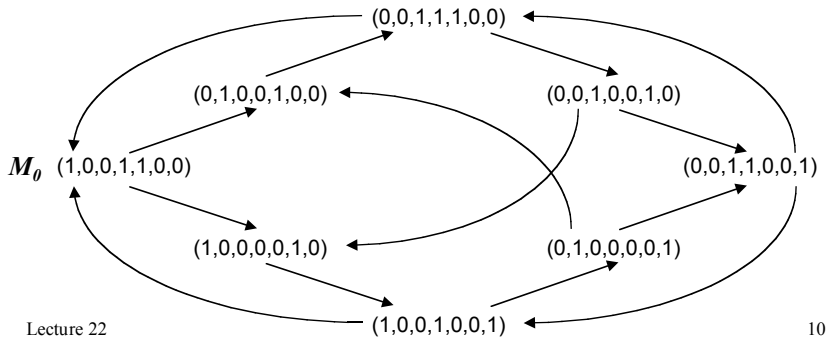
$$\boldsymbol{M} = (|\mathbf{In_1}|, |\mathbf{CR_1}|, |\mathbf{Out_1}|, |\mathbf{Sem}|, |\mathbf{In_2}|, |\mathbf{CR_2}|, |\mathbf{Out_2}|)$$
$$= (0,1,0,0,0,1,0)$$

Reachability Graph

Each node in the graph is a marking
$(|\mathbf{In_1}|, |\mathbf{CR_1}|, |\mathbf{Out_1}|, |\mathbf{Sem}|, |\mathbf{In_2}|, |\mathbf{CR_2}|, |\mathbf{Out_2}|)$

Reachability Graph

Each node in the graph is a marking
$(|\mathbf{In_1}|, |\mathbf{CR_1}|, |\mathbf{Out_1}|, |\mathbf{Sem}|, |\mathbf{In_2}|, |\mathbf{CR_2}|, |\mathbf{Out_2}|)$



Petri Net Dynamic Analysis

- Example: Two-process Semaphore

  Is it possible for both processes to be in their critical regions at the same time in the same marking? That is, is the following a valid marking?

$$\boldsymbol{M} = (|\mathbf{In_1}|, |\mathbf{CR_1}|, |\mathbf{Out_1}|, |\mathbf{Sem}|, |\mathbf{In_2}|, |\mathbf{CR_2}|, |\mathbf{Out_2}|)$$
$$= (0,1,0,0,0,1,0)$$

Static Analysis

- Goal: Prove Theorems About Properties
- An Analysis Characterizes a Class of Behaviors
- Applied to a (Static) Model
- Can Abstract Away Critical Apsects
- In General, Impossible to Prove Absence of Error

Petri Net Static Analysis

- The Method of Invariants

  Invariants are properties of a Petri net that hold in all markings

- Analysis Cast as Proof of Invariance

Petri Net Static Analysis

- Example: Two-process Semaphore

  Is the sum of the tokens in $\mathbf{CR_1}$, $\mathbf{CR_2}$, and **Sem** equal to 1 in all reachable markings? That is,

  $\Box \quad |\mathbf{CR_1}| + |\mathbf{CR_2}| + |\mathbf{Sem}| = 1$