Introduction to verifying concurrent systems using SPIN

Behrouz Talebi

Concurrent Programming LP1 2014

What is SPIN?

What is SPIN?

- The SPIN model checker is a software tool for specifying and verifying concurrent and distributed systems

What is SPIN?

- The SPIN model checker is a software tool for specifying and verifying concurrent and distributed systems
- It uses the programming language **Promela** to write the models

What is SPIN?

- SPIN looks for counterexamples showing that the program breaks the spec.
  - no counterexample = correct!
  - If the state-space is too large, it will not terminate (timeout)

SPIN’s relation to this course?

SPIN’s relation to this course?

- Write programs from the book in Promela

SPIN’s relation to this course?

- Write programs from the book in Promela
- Check for mutex, deadlocks and liveness...

SPIN's relation to this course?

- Write programs from the book in Promela
- Check for mutex, deadlocks and liveness...
- We use assertions or LTL formulas
  - assert a safety property at a point in the program:
    assert(count == n)
    - *What if the program never gets there?*
  - LTL formulas express properties about future states
    - (e.g., absence of deadlock, and liveness)

SPIN's relation to this course? 2

- Not required for the exam
- But may help to make proofs more concrete
  - Helps understand formal logic
  - SPIN can confirm your informal proofs
    - Help you understand when a "proof" really is a proof and when it is handwaving
  - Use it for exercises in the book!
- Formal logic is a small part of the exam (⅙)
  - SPIN helps you practice with this

How to use SPIN

- The official SPIN webpage: http://spinroot.com/spin/whatispin.html

- The web interface for SPIN by Bart van Delft webpage: **http://abu.se.informatik.tu-darmstadt.de/sefm/spin/**