Analysis of Software Artifacts

SMV continued (Lecture 6)
we will not cover this material in tests or homeworks

home page

today we will briefly discuss SPIN and Verisoft

look at other model checkers on the formal methods

overview of other model checkers
• Please get a copy of the paper cited above
• Pages 279-297, May 1997
  Transactions on Software Engineering, Vol 23, No 5,
  C.J. Holzman, The Model Checker SPIN, IEEE
• Developed at Bell Labs by Gerhard Holzmann

SPIN
any combination of these shared variables –
through message passing on buffered channels –
communication between processes ●

asynchronous composition of processes ●

based on CSP, but much more user-friendly ●
called PROMET (a Process Meta Language) ●

SPIN (Modeling Language)
What does the following formulas say?

- Use \( \cup \) for union.
- Use \( \cap \) for intersection.
- Use \( [ ] \) for concatenation.
- Linear Time Temporal Logic (LTL).

SPIN (Specification Language)
counterexample animation

message passing

modeling language more natural for certain systems

nice GUI

Advantages over SMV
constantly being improved •
pretty big user community •
in general, can handle larger systems •

Advantages of SMV