SMV continued (Lecture 6)

Analysis of Software Artifacts

Agenda

- overview of other model checkers

- look at other model checkers on the formal methods home page

- today we will briefly discuss SPIN and Verisoft

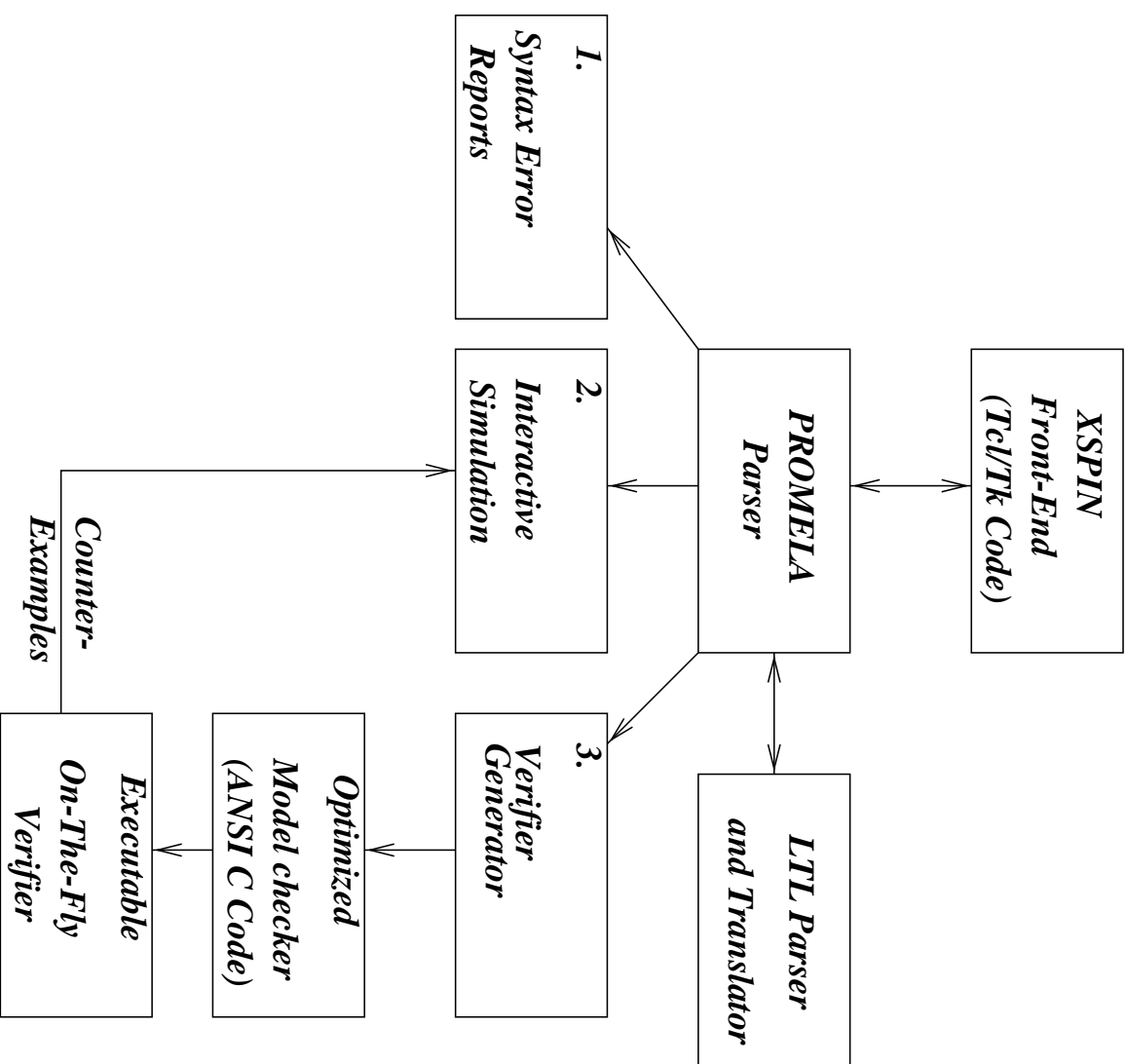- we will not cover this material in tests or homeworks

SPIN

- developed at Bell labs by *Gerard Holzmann*

- G.J. Holzmann, *The Model Checker SPIN*, IEEE Transactions on Software Engineering, Vol 23, No 5, pages 279-295, May 1997

- please get a copy of the paper cited above

SPIN (Modeling language)

- called PROMELA (a Process Meta Language)

- based on CSP, but much more *user friendly*

- asynchronous composition of processes

- communication between processes

  – through message passing on buffered channels

  – shared variables

  – any combination of these

- *Linear Time Temporal* logic or LTL.

- — Use [] for **G**

  — Use <> for **F**

  — use U for **U**

- what does the following formulas say?

  — ![](sr -> <> rr)

  — (!rr U rb)

XSPIN Front-End (Tcl/Tk Code)

PROMELA Parser

LTL Parser and Translator

1. Syntax Error Reports

2. Interactive Simulation

3. Verifier Generator

Optimized Model checker (ANSI C Code)

Executable On-The-Fly Verifier

Counter-Examples

Advantages over SMV

- nice GUI

- modeling language more natural for certain systems

  - message passing

- counterexample animation

Advantages of SMV

- in general, can handle larger systems

- pretty big user community

- constantly being improved