Formal Methods in Software Development
Resume of the 28/10/2020 lesson

Igor Melatti and Ivano Salvo

1 The SPIN model checker

- Another *explicit* model checker
- Verification algorithm conceptually similar to the Murphi one
- Input language much different, actually more complicated
  - we more or less saw the whole Murphi input language
  - we will be able to actually study only the main aspects of SPIN input language
  - for all details, see `http://spinroot.com/spin/Man/promela.html`
  - Murphi input language does not have a name; SPIN input language does have: Promela, standing for "PROcess MEta LAnguage"
  - there is a book dealing with SPIN, Promela and their usage only:: Gerard J. Holzmann, "The SPIN Model Checker: Primer and Reference Manual", Addison-Wesley Professional, 2004
- SPIN stands for "Simple Promela INterpreter"
- SPIN is especially tailored for protocols verification, as it is based on process parallel execution
  - SPIN mostly targets interleaving between processes
  - Murphi tries to exploit symmetries
- See slides by Ruys