Formal Methods in Software Development
Exercise 1 (October 27)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.uni-linz.ac.at

October 12, 2008

The result is to be submitted by the deadline stated above via the Moodle interface as a .zip or .tgz file which contains

- A PDF file with
  - a cover page with the title of the course, your name, Matrikelnummer, and email-address,
  - for each exercise, a section with the number and name of the exercise and a copy of the ProofNavigator file used in the exercise,
  - for each proof of a formula F, a screenshot of the RISC ProofNavigator after executing the command `proof` F,
  - optionally any explanations or comments you would like to make;
- the RISC ProofNavigator (.pn) files used for the proofs;
- the proof directories generated by the RISC ProofNavigator.

Exercise 1: RISC ProofNavigator

Take the file "exercise1.pn" and use the RISC ProofNavigator to prove the formulas A, B, C, D, and M, in this file.

The formulas A–D are simple predicate logic proofs that only require the commands `scatter`, `split`, and `instantiate`.

> Rather than `instantiate`, you may also first try `auto`; the submitted proofs, however, must *not* make use of the `auto` command. Please also try the repeated application of the command `flatten` (rather than `scatter`) to see the gradual decomposition of the proof.

Formula M can be proved by `induction`, `scatter`, and several (in the induction step three) applications of `instantiate` (`auto` must not appear in the proof).