

Formal Methods in Software Development

Exercise 0 (March 29)

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

March 12, 2007

The result is to be submitted to me by **March 29** (hard deadline) as an email that includes as attachments both the ProofNavigator file (`exercise0.pn`) and the zipped version of the generated directory “`exercise0`” containing the proofs (`exercise0.zip` or `exercise0.tgz`).

Questions can be asked per email or in the classes before the deadline.

1 The RISC ProofNavigator

Warmup Training (Mandatory, 5 points) On the web site, you find a file “`exercise0.pn`”. Use the RISC ProofNavigator to prove the formulas A, B, C, D, E, T1 in this file.

The formulas A–E 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 T1 can be proved by `induction` and `instantiate` (again, `auto` must not appear in the proof).

Induction Proofs (Voluntary, 5 points) Formula T2 can be proved by `induction`, `scatter`, `auto`, `instantiate` (the proof of the induction step requires up to 3 manual instantiations).

Formula T3 can be proved similar to T2 but requires two applications of command `lemma`: in the induction base, T1 has to be imported as a lemma; in the induction step, T2 has to be imported.