Formal Methods in Software Development
Exercise 1 (April 3)

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

March 15, 2006

The result is to me submitted to me by **April 3** (hard deadline) as an email that includes as an attachment both the PVS file (.pvs) and the corresponding proof file (.prf).

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

1 PVS Training

On the Web site you find a PVS file "exercise1.pvs". Use PVS to prove the lemmas A, B, C, D, E, T, S in this file.

The lemmas A–E are simple predicate-logic proofs that only require the PVS commands `skolem!`, `inst`, `flatten`, `split`, and `assert`. The use of the `grind` command is *not* allowed.

Lemma T can be proved by an additional (single) use of the `expand` command (please note that `(expand` *`name num pos`*`)` expands occurence number *pos* of name *name* in formula number *num*).

Lemma S can be proved by induction on one of its arguments (command `induct`).

I strongly suggest that you try these proofs as soon as possible (not tomorrow, NOW!) such that you get familar with PVS.