SFWR 2F03 Assignment 5 - Part 1: Partial Functions & Typechecking in PVS

Due: 1730 Wednesday December 4, 1998

For this assignment you will do all your PVS work in a single file containing multiple theories. Use netscape to download the file “Assignment5.dmp” from the Notes directory of the course home page:

http://www.cas.mcmaster.ca/ lawford/2F03/Notes/

Undump the file and then open the file “Assignment5.pvs”.

1. Predicate Subtypes in PVS

   a) Prove each of the three theorems in the theory “colors”. The first two can be proved using (SKOLEM!), (FLATTEN) and (ASSERT). Try using these commands to prove the theorem “red_or_yellow”. To finish this proof you need to introduce predicate subtype information using the command (TYPEPRED ”t_1”), where t_1 is the appropriate term.

   b) What is the simplest PVS strategy (command) that could be have been used to complete the proof of “red_or_yellow” in a single proof step? Use it on “red_or_yellow”.

2. Stupid PVS Tricks Part II (The Danger of AXIOMs: “Proving” $1 = 2$)

   PVS allows you to define axiomatic theories with the AXIOM declaration. In PVS axioms are like premises that can be brought into a proof at any point with the command:

   ```
   (LEMMA "ax_name")
   ```

   The theory “inconsistent” in the file contains the AXIOM “bad”. Use “bad” to prove theorems P1, P2 and P3.

   While “bad” is a misstatement of *modus ponens* and obviously inconsistent, in theories containing more complicated sets of axioms, it is often difficult or impossible to verify the consistency of the axioms. For this reason PVS documentation encourages the user to employ axioms sparingly and instead use definitions where ever possible.

3. Proofs with equality

   a) Use PVS to do Rubin Ch. 11, p. 244 E 11. Do this by creating a theory called equal11 in your file containing appropriate definitions and a theorem called E11. Using a combination of (BDDSIMP), (SKOLEM!) and (INST?) you should be able to reduce E11 to a single sequent that requires the use of the PVS equivalent of Rubin’s Rule I part (b) Substitution of Equals. This is the PVS command

   ```
   (REPLACE -n * LR)
   ```

   Here equation -n in the premises is of the form $t_L = t_R$. In this case the above command makes all valid substitutions of t_R for t_L in all other formulas of the sequent. Changing the argument LR with RL would replace right-to-left, performing all valid substitutions of t_L for t_R.

   b) Putting the above commands together into a *proof strategy* would complete the above proof in a single step. The PVS commands (GRIND) and (GRIND$) do all this and more (e.g. they also uses (LIFT-IF)). The $ version expands out all the proof steps whereas regular (grind) just records itself as a single step. Make a copy of theorem E11 and rename it “E11b”. Prove the theorem “E11b” with the single command “(GRIND)”.

   c) Do a formal proof of question E11 by hand.

   d) Create a new theory called “equal9” containing the theorem “E9” for Rubin p. 242 E9. Use the (GRIND$) command to reduce E9 to an unprovable sequent. Write down the characteristic formula for the sequent. Create an interpretation structure **S** with a two element universe that makes the characteristic formula false. Confirm that the interpretation structure also proves that the argument in E9 is invalid.

4. Partial functions in logic

   Write down formulas in both the IMPS/Parnas (analysis style) logic and bounded quantification (PVS style) logic that would be satisfied by A, an array of integers, for the following properties:

   a) The array contains a decreasing sequence of elements.

   b) The array contains a decreasing sequence of elements and there are no repeat elements.

Part 2 of Assignment 5 will be given out shortly. It will require you to do more work in the Assignment5.pvs file. DO NOT SUBMIT A DUMP FILE OF YOUR WORK UNTIL YOU HAVE ALSO COMPLETED PART 2.