SFWR ENG 2F04 Assignment 4: More Predicate Logic + PVS

Due: 1230 Thursday November 18, 1999

All of your PVS work for this assignment should be done in a single file called `A4.pvs` (note the capital "A"). You will submit your PVS work electronically as a PVS dump file called `A4.dmp`. Written work will be handed in separately at the *start* of class on the due date. NOTE: For the latest missive on how to submit your PVS work to your great oppressors, please check out the URL:

`http://www.cas.mcmaster.ca/~lawford/2F04/e-submissions.html`

1. Download the file A4.dmp from the URL:

   `http://www.cas.mcmaster.ca/~lawford/2F04/Notes/A4.dmp`

   Undump the file and then open A4.pvs. Make sure that you switch contexts to the directory where you undump the file with the PVS/Context/change-context command. Use the PVS/Prover Invocation/x-step-proof menu command on theorems `IbEx` and `E11` to step through the proofs of these theorems and see how the commands work.

2. (30 marks) Now use PVS to do Rubin Ch. 9, p. 199 B 5, 11, 15; D 3, 6, 7 and Ch. 10 p. 222 B 23, 25. For each question create a new theory with the PVS/Files and Theories/new-theory command. As was done for the 2nd example theory in the file, name each new theory and main theorem in the following format: theory `ch9B9` for Chapter 9 question B9 and THEOREM name `B9`, etc.

   Note: To do some of the above, you may need to use (INST * "t_1" "t_2"), the multi-variable version of INST to deal with the equation of the form $(\forall x)(\forall y)\phi$ in the premises or $(\exists x)(\exists y)\phi$ in the conclusions. This is similar to doing a multi-variable version of Rule US or EG respectively in a hand proof.

3. (30 marks) Do the questions from Rubin found in 2 above by hand.

4. Retrieving a formula from the great beyond (a.k.a. using hidden formulas).

   You will use PVS to prove:

   $$\vdash (\forall x)Px \rightarrow Pa \wedge Pb$$

   To do this create a new theory called `a4Q4`.

   a) (5 marks) Create the required definitions and a new THEOREM called Q4 in you file and start the proof. After you have used (INST * "a") at one point in your proof, use the PVS "show-hidden-formulas" command from the "Proof Information" submenu to show the "hidden" formulas. Bring the formula back into the sequent with the command (REVEAL -1) and finish the proof.

   b) (5 marks) Let $\phi[t|x]$ be a valid substitution. Explain why $(\forall x)\phi \vdash \psi$ iff $(\forall x)\phi, \phi[t|x] \vdash \psi$

5. (99 Final) Understanding PVS commands in terms of Natural Deduction Rules of Inference:

   a) (5 marks) Consider the application of the PVS (SKOLEM!) command show below:

   $$\dfrac{\begin{array}{l}\phi_1\\ \phi_2\\ \vdots\end{array}}{(\forall x)\psi} \quad \underset{\Longrightarrow}{\text{(SKOLEM!)}} \quad \dfrac{\begin{array}{l}\phi_1\\ \phi_2\\ \vdots\end{array}}{\psi[x_1|x]}$$

   Here x_1 is a new variable not occurring elsewhere in the sequent. PVS is saying, in effect, that to prove $\Gamma \vdash (\forall x)\psi$, it is *sufficient* to prove $\Gamma \vdash \psi[x_1|x]$ for an appropriately chosen x_1. Why?

b) (5 marks) Using what you know about Logical Equivalence (Rule LE) and how PVS handles negations, show how the above explanation also covers the use of the PVS (SKOLEM!) command in the case where:

$$\begin{array}{l} \phi_1 \\ \phi_2 \\ \vdots \\ (\exists x)\phi \\ \hline \psi_1 \\ \psi_2 \\ \vdots \end{array} \quad \underset{\Longrightarrow}{\text{(SKOLEM!)}} \quad \begin{array}{l} \phi_1 \\ \phi_2 \\ \vdots \\ \phi[x_1|x] \\ \hline \psi_1 \\ \psi_2 \\ \vdots \end{array}$$

Use intermediate sequents to illustrate the process and provide justification for the transformation of one sequent to the next.

6. Proofs with equality

a) (5 marks) Do a formal proof of question Rubin p. 244 E11 by hand.

b) (4 marks) Create a new theory called "ch11E9" containing the theorem "E9" for Rubin p. 242 E 9. Use the usual PVS commands 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.

7. (Final'99) In the following you will deduce some properties of a world where there are winners and losers (those who did not win).

i) (7 marks) Formally prove:

$$(\exists x)Wx, (\exists x)\neg Wx \vdash (\forall x)(\exists y)x \neq y$$

ii) (2 marks) What do you conclude about the cardinality of the universe for any interpretation structure satisfying the two premises?

iii) (2 marks) Find the simplest interpretation structure (i.e. having the smallest universe) that is a model for the formula:

$$(\exists x)Wx \wedge (\exists x)\neg Wx \rightarrow (\forall x)(\exists y)x \neq y$$