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

Due: 1130 Tuesday November 21, 2000

For this assignment you may work in pairs on the PVS part of the assignment but you must work alone on the write-up and proofs by hand.

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

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. **Fill in the requested info in the table at the top of the file.**

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.

1. **PVS Predicate Logic** (30 marks)

   Use PVS to do Rubin Ch. 9, p. 199 B 2, 8, 14; D 2, 5, 10 and Ch. 10,p. 222 B 10, 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.

2. **Manual Practice** (30 marks)

   Do the questions from Rubin found in 1 above by hand.

3. **Retrieving a formula from the great beyond (a.k.a. using hidden formulas)** (15 marks)

   You will use PVS to prove:

   $$\vdash Pf(a) \vee Pb \rightarrow (\exists x)Px$$

   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 with the `(FLATTEN)` command. Next use `(INST * ''f(a)'')`
   Now 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 $\psi \vdash (\exists x)\phi$ iff $\psi \vdash (\exists x)\phi \vee \phi[t|x]$

   c) (5 marks) While `(inst ...)` deals with existential quantifiers in the conclusion, `(SKOLEM!)` "eliminates" existential quantifiers in the premises. Consider the application of the PVS `(SKOLEM!)` command show below:

   $$\left|\begin{array}{c} \phi_1 \\ \phi_2 \\ \vdots \\ (\exists x)\phi \\ \hline \psi_1 \\ \psi_2 \\ \vdots \end{array}\right. \quad \overset{\text{(SKOLEM!)}}{\Longrightarrow} \quad \left|\begin{array}{c} \phi_1 \\ \phi_2 \\ \vdots \\ \phi[x_1|x] \\ \hline \psi_1 \\ \psi_2 \\ \vdots \end{array}\right.$$

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

4. **Proofs with equality** (10 marks)

   a) (5 marks) Do a formal proof of question Rubin p. 244 E10 by hand.

   b) (5 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.

5. **More Predicate Logic with Equality** (15 marks - From the 1999 Final)

   Any function $f : U \to U$ induces an equivalence relation K_f, the *equivalence kernel of* f, given by

   $$K_f xy \text{ if and only if } f(x) = f(y).$$

   a) (6 marks) In this question you will formally prove that given a function $f : U \to U$, the equivalence kernel of f is an equivalence relation. To do this, formally prove the following:

   i) Reflexivity: $(\forall x)K_f xx$,

   ii) Symmetry: $(\forall x)(\forall y)(K_f xy \to K_f yx)$,

   iii) Transitivity: $(\forall x)(\forall y)(\forall z)(K_f xy \wedge K_f yz \to K_f xz)$.

   b) (2 marks) We can define a partial order on equivalence relations as follows: Let E_1 and E_2 be equivalence relations on U. Then we say that E_1 is a refinement of E_2, written $E_1 \preceq E_2$ iff $(\forall x)(\forall y)(E_1 xy \to E_2 xy)$.

   Given functions $f : U \to U$ and $g : U \to U$, write down a predicate logic formula involving the function symbols f and g that is true when $K_g \preceq K_f$).

   c) (5 marks) Consider the following result from discrete mathematics:

   Theorem: Given two functions with the same domain, $f : V_1 \to V_3$ and $g : V_1 \to V_2$, then there exists $h : V_2 \to V_3$ such that the diagram in Figure 1 commutes iff $K_g \preceq K_f$.

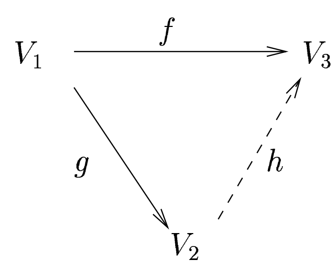

Figure 1: Commutative diagram for $(\exists h : V_2 \to V_3)(\forall v_1 \in V_1)[h(g(v_1)) = f(v_1)]$ iff $K_g \preceq K_f$

   The interpretation of this result is that for h to exist, g must retain as much or more information about its domain than f.

   You will now show that $K_g \preceq K_f$ is a necessary condition for the existence of the function h in the special case when $V_1 = V_2 = V_3$ by formally showing the following result:

   $$\vdash (\forall x)[f(x) = h(g(x))] \to (\forall x)(\forall y)[g(x) = g(y) \to f(x) = f(y)]$$

   d) (2 marks) Use the previous result to show that:

   $$\models (\exists x)(\exists y)(g(x) = g(y) \wedge f(x) \neq f(y)) \to (\exists x)(f(x) \neq h(g(x))$$