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

Due: 1720 Tuesday November 12, 2002

All of your PVS work for this assignment should be done in a single file called `a4.pvs` in a subdirectory where you want to keep your 2F04 PVS material. For this assignment, to receive credit for your PVS work in question 2, you must demonstrate your PVS work in the lab to a TA. Your written work can be handed in as usual at the end of your tutorial on the due date.

To help you get started, download the file a4.dmp from the URL: `http://www.cas.mcmaster.ca/~lawford/2F04/Notes/a4.dmp` Undump the file with the `PVS/FilesandTheories/undump-pvs-files` command and then open the file `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/ProverInvocation/x-step-proof` menu command on theorems `IbEx` and `E11` to step through the proofs of these theorems buy typing $< tab >$ then $< 1 >$ (the tab key, then the "1" key). This will show you have the commands work.

For each of the PVS questions below, create a new theory with the `PVS/FilesandTheories/new-theory` command. Name each new theory and main theorem in the following format: theory `q2a` for Assignment question 2(a), `q2b` for question 2(b), etc.

1. Predicate Logic Proofs

Do the following questions from Huth+Ryan by hand.

a) p. 111 1, 2, 3

b) p. 125 1(e)(g). For both of these questions, try to prove the result in the other direction, i.e., attempt a proof from the conclusion to the premise. If a proof does not exist, create a model that demonstrates that no proof exists.

c) p. 126 4

d) p. 127 7(d)

2. PVS Predicate Logic

Use PVS to do help determine if the following arguments are valid. If the arguments are not valid, create a counter example, a model $\mathcal{M}$ such that $\mathcal{M} \models \phi_i$ for each premise ϕ_i and $\mathcal{M} \not\models \psi$ for the conclusion ψ.

a)

$$\forall x(P(x) \to \neg Q(x)), \forall x(Q(x) \vee \neg R(x)), \exists x \neg Q(f(x)) \vee \exists x Q(f(x)) \vdash \exists x(\neg P(f(x)) \vee \neg R(f(x)))$$

b)

$$\exists x[E(x) \wedge \forall y(F(y) \to G(x,y))], \forall x \forall y[E(x) \to (G(x,y) \leftrightarrow H(y))] \vdash \forall x(F(x) \leftrightarrow H(x))$$

c) Let a and b be constants.

$$\neg\exists x(P(x) \wedge \neg R(x)), \neg\exists x(Q(x) \wedge R(x)), P(a), Q(b), a = b \vdash \bot$$

d)

$$\forall x \exists y(R(x,y) \to R(y,x)), \exists x(P(x) \wedge \neg R(x,x)), \exists x \forall z(x \neq z \to \neg P(x) \wedge R(z,x) \wedge R(x,z)) \vdash \bot$$

3. Do formal proofs of by hand of 2(a) and (c) above.

4. More Predicate Logic with Equality (15 marks on the 1999 Final)

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

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

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

i) Reflexivity: $\forall x K_f(x, x)$, i.e., show $\vdash \forall x(f(x) = f(x))$

ii) Symmetry: $\forall x \forall y(K_f(x, y) \to K_f(y, x))$, i.e., show $\vdash \forall x \forall y(f(x) = f(y) \to f(y) = f(x))$,

iii) Transitivity: $\forall x \forall y \forall z(K_f(x, y) \wedge K_f(y, z) \to K_f(x, z))$, i.e., show

$$\forall x \forall y \forall z(f(x) = f(y) \wedge f(y) = f(z) \to f(x) = f(z))$$

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

Given functions $f : A \to A$ and $g : A \to A$, 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 $K_g \preceq K_f$.

$$\begin{tikzcd}
V_1 \arrow[rr, "f"] \arrow[dr, "g"'] & & V_3 \\
& V_2 \arrow[ur, dashed, "h"'] &
\end{tikzcd}$$

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:

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