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

Due: 0830 Thursday November 25, 2004

1. Predicate Logic Proofs

Do the following questions from Huth+Ryan by hand.

a) Huth+Ryan 2nd Ed. p. 160 Exercises 2.3: 1, 2, 3
[Note: For those of you with the 1st edition, this corresponds to: p. 111 1, 2, 3]

b) Huth+Ryan 2nd Ed. p. 161 Exercises 2.3: 9(l)(n)(p)
[Huth+Ryan 1st Ed.p. 125 1(e)(g) 7 (d)].
For the first two parts ((l) and (n)) of this question, 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) Huth+Ryan 2nd Ed p. 161 7
[Huth+Ryan 1st Ed p. 126 4]

2. PVS Predicate Logic

You will submit your PVS files using the subversion revision control system at:

`https://websvn.mcmaster.ca`

Use your CAS login id and your CAS password to access the system.

Login to one of the CAS systems with subversion (`svn`) and PVS (`pvs`) installed. Then do the following:

```
svn checkout https://websvn.mcmaster.ca/trunk/se2f03/YOUR_CAS_LOGIN/Assignment4
```

For me `YOUR_CAS_LOGIN` is replaced by `lawford`. This will create a subdirectory named `Assignment4`. Then do the following:

```
cd Assignment4
pvs a4.pvs
```

Whenever you want to leave your work, check it into the revision control system with the `svn commit` command. For example, in your working directory type:

```
svn commit -m "Completed Question 2a.  Question 2b started but incomplete."
```

You can then pull down the latest version of your files and continue your work on any system with PVS and subversion by repeating the above process on another machine or use the `svn update` command in the `Assignment4` directory.

When you are done your PVS work you, first make sure you commit the changes to the revision control system.

```
svn commit -m "Completed Assignment 4 PVS work."
```

Finally, to submit the files for marking, you must "tag" your submission with the following command:

```
svn copy https://websvn.mcmaster.ca/trunk/se2f03/YOUR_CAS_LOGIN/Assignment4 \
https://websvn.mcmaster.ca/tags/se2f03/YOUR_CAS_LOGIN/Assignment4 \
-m "Tagging Assignment 4 for marking."
```

Use the `PVS/ProverInvocation/x-step-proof` menu command on theorems `IbEx` and `E11` to step through the proofs of these theorems by typing $< tab >$ then $< 1 >$ (the tab key, then the "1" key). This will show you how the commands work.

For each of the PVS questions below, create a new theory with the `PVS/Files and Theories/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.

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)

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

b)

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

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)

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

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

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

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

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 $\forall x \forall y(E_1(x,y) \rightarrow E_2(x,y))$.

Given functions $f : A \rightarrow A$ and $g : A \rightarrow A$, 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, $f : V_1 \rightarrow V_3$ and $g : V_1 \rightarrow V_2$, then there exists $h : V_2 \rightarrow V_3$ such that the diagram in Figure 1 commutes 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:

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

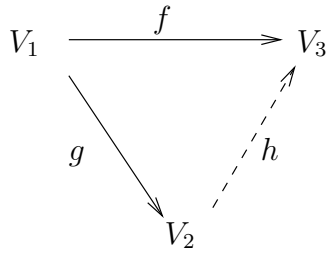

Figure 1: Commutative diagram for $(\exists h : V_2 \to V_3)(\forall v_1 \in V_1)[h(g(v_1)) = f(v_1)]$ iff $K_g \preceq K_f$

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

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

5. More Textbook Practice Questions

a) Huth+Ryan 2nd Ed. Ex 2.2 p. 158-159 1, 3, 5, 6
[Huth+Ryan 1st Ed. p. 101 1, 3, 5, 6]

b) Huth+Ryan 2nd Ed. Ex 2.2 p. 158-159 4, 5
[Huth+Ryan 1st Ed. p. 108 1, 2]

c) Huth+Ryan 2nd Ed. Ex 2.4 p. 163-164 1, 3, 4, 5
[Huth+Ryan 1st Ed. p. 135 1, 3, 4, 6]

d) Huth+Ryan 2nd Ed. Ex 2.4 p. 163-164 6, 8, 10, 11, 12(a)(b)(g)
[Huth+Ryan 1st edition: p. 139 1, 2, 5, 6, 8(a)(b)(g)]

6. Predicate Logic Models (from 2002 final)

a) Consider the following sequence of formulas:

$$\begin{aligned} \Gamma \;:=\; & \exists x \forall y \neg Q(x,y), \\ & \exists x (Q(x,x) \wedge \forall y (Q(y,y) \to x = y)), \\ & \exists x \exists y \exists z (Q(x,y) \wedge Q(x,z) \wedge y \neq z), \\ & \forall x (f(x) = x \to \exists y Q(y,x)) \end{aligned}$$

The intended interpretation for these formulas is a FSM model $\mathcal{M}$ where:

$$\begin{aligned} A \;&:=\; \{a,b,c,d,e\} \text{ is the universe, the finite set of states} \\ f^{\mathcal{M}}(x) \;&:=\; a \text{ is the reset function that returns the FSM to the initial state } a, \end{aligned}$$

and the interpretation of Q, denoted $Q^{\mathcal{M}}$, is the FSM transition relation yet to be determined.
In your summer job as a software developer you are given Γ as a formal specification and told to create two different versions of the transition relation $Q^{\mathcal{M}}$.

i) (3 marks) First, find a $Q^{\mathcal{M}}$ such that for this interpretation of Q we have $\mathcal{M} \not\models \Gamma$.

ii) (7 marks) Next, find a different $Q^{\mathcal{M}}$ such that for this interpretation of Q we have $\mathcal{M} \models \Gamma$.

b) Consider the new sequence of formulas:

$$\begin{aligned} \Gamma' \;:=\; & \exists x \forall y \neg Q(x,y), \\ & \exists x (Q(x,x) \wedge \forall y (Q(y,y) \to x = y)), \\ & \exists x \exists y \exists z (Q(x,y) \wedge Q(x,z) \wedge y \neq z), \\ & \forall x (f(x) = x \to \exists y Q(y,x)), \\ & \forall x \forall y \forall z (Q(x,y) \wedge Q(x,z) \to y = z) \end{aligned}$$

c) (10 marks) Determine if Γ' is inconsistent. Note: Informal arguments are not acceptable. Only a formal proof or a model will be accepted.

d) (5 marks) Based upon your answer to the previous question, does there exists a graph that provides a model $\mathcal{M}$ such that $\mathcal{M} \models \Gamma'$? Draw the graph or explain why no such graph exists.