SFWR ENG 2F03 Assignment 3: More Propositional PVS & Predicate Logic Syntax & Interpretations

Due: 0830 Thursday October 21, 2004

Preface

Your written answers to the questions below should be handed in in class.

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 co https://websvn.mcmaster.ca/trunk/se2f03/YOUR_CAS_LOGIN/Assignment3
```

For me `YOUR_CAS_LOGIN` is replaced by `lawford`. This will create a subdirectory named `Assignment3`. Then do the following:

```
cd Assignment3
pvs a2.pvs
```

When ever 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 Questions 1 and 2.  Question 3 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.

When you are done your PVS work you, first make sure you commit the changes to the revision control system. Finally, to submit the files for marking, you must "tag" your submission eiwith the following command:

```
svn copy https://websvn.mcmaster.ca/trunk/se2f03/YOUR_CAS_LOGIN/Assignment3 \
https://websvn.mcmaster.ca/tags/se2f03/YOUR_CAS_LOGIN/Assignment3 \
-m "Tagging Assignment 3 for marking."
```

The Questions

1. In PVS when when you are asked to find a proof of the form $\Gamma, \neg\phi \vdash \psi$, the `(FLATTEN)` command changes this into a proof obligation of the form $\Gamma \vdash \phi \vee \psi$

   Use the proof rules from Huth+Ryan to show why if $\Gamma \vdash \phi \vee \psi$, then $\Gamma, \neg\phi \vdash \psi$.

2. A sequence of premises Γ is *inconsistent* if $\Gamma \vdash \bot$. In this case, by soundness of our proof system $\Gamma \models \bot$ which tells us that there are no rows in the truth table for Γ where all of the premises are true (i.e., it is impossible to simultaneously satisfy all of the premises). On the other hand, we say that the sequence of premises Γ is *consistent* if $\Gamma \not\models \bot$, i.e., there is at least one row of the truth table where all of the premises are true. In this case, by the completeness of out proof system we have $\Gamma \nvdash \bot$ (i.e. no proof of $\bot$ from Γ exists).

   Use PVS to determine if Γ is inconsistent for

Continued on page 2

a)

$$\Gamma := a \wedge c \rightarrow d, b \wedge c \rightarrow d, \neg(a \vee b) \rightarrow e \vee f, g \rightarrow \neg e, \neg f \vee h, c \wedge \neg d, g \rightarrow h$$

Call this `Q2a: PROPOSITION` ....

b)

$$\Gamma := a \rightarrow (b \rightarrow c), \neg a \rightarrow d \wedge \neg e, a \wedge b \rightarrow \neg c, d \rightarrow f \vee g, b \vee (g \rightarrow h), g \rightarrow e \vee h, g \wedge \neg h$$

Call this `Q2b: PROPOSITION` ....

In any cases when the proof of $\Gamma \vdash \bot$ fails, write down the characteristic equation of one of the unprovable sequents, determine a truth assignment that falsifies the characteristic equation and then use that to obtain a row in the truth table that shows that $\Gamma \not\models \bot$.

3. **a)** In the file `a2.pvs`, write down a PVS theorem called `Q3a` that you would attempt to demonstrate that the following argument is valid:

$$p \rightarrow q, \neg(q \wedge \neg r), p \models r$$

b) Invoke the PVS prover on the theorem you stated in part (c), apply the (FLATTEN) command. You should obtain the sequent:

```
{-1}    (p IMPLIES q)
{-2}    p
  |-------
{1}     (q & NOT r)
{2}     r

Rule?
```

Show the step-by-step sequent transformations done by the (FLATTEN) command to transform your original theorem statement into the current sequent. Justify each step using our proof rules, tautologies, valid arguments and properties of sequents.

c) Recall that PVS effectively does the proofs in reverse. Thus PVS is saying that to show

$$p \rightarrow q, \neg(q \wedge \neg r), p \vdash r \tag{1}$$

begin by showing

$$p \rightarrow q, p \vdash (q \wedge \neg r) \vee r \tag{2}$$

Suppose that on line n of your proof you have shown (2). Show what the next lines of a formal proof would be to use this to show (1) on line $n + k$.

d) Apply the PVS command (SPLIT -1) to the first equation in the premises of the sequent in (b). What sequents result and why is one of them trivially true? Finish the proof using whatever PVS commands you desire.

e) Do a formal proof of the valid argument by hand i.e., show

$$p \rightarrow q, \neg(q \wedge \neg r), p \models r$$

by showing that

$$p \rightarrow q, \neg(q \wedge \neg r), p \vdash r$$

Continued on page 3

f) Make a copy of theorem `Q3a` and rename it `Q3f`. Modify `Q3f` to check the validity of the argument

$$p \rightarrow q, \neg(q \wedge \neg s), p \models r$$

Attempting to prove `Q3f` should result in an unprovable sequent. Write down the characteristic equation for this unprovable sequent and find a counter example that makes the equation false.

g) Write down and prove a theorem called `Q3g` that demonstrates that the counter example from (g) satisfies all of the premises, but does not satisfy the conclusion r. What do you conclude about the validity of the argument

$$p \rightarrow q, \neg(q \wedge \neg s), p \overset{?}{\models} r$$