Lab 5: PVS Basic Specifications

JSO

EECS, LSE

October 15, 2018

Table of contents

1. Preparation from Last week's PVS Introduction Lab (Lab4)
2. To Do
   - Predicate Logic
   - Majority Vote
   - Telephone book
3. To Submit

Preparation from Last week: Precondition for this Lab

- Completion of previous PVS Introductory Lab4. Also see: `http://pvs.eecs.yorku.ca/`, *Getting started with PVS*)
- WIFT Readings (see PVS/WIFT tutorial, especially the telephone book: `http://bit.ly/2cnawwN`)
- Propositional Logic and Set Theory (See: `http://bit.ly/2cnawwN`).
- This week's lectures on using propositional and predicate logic for Specifications
- Ensure that you know the proof rules for quantifier elimination.
- Ensure that you can do proofs by induction (needed for a theorem involving a recursive function).
- Study the WIFT Tutorial telephone book specfication

Predicate Logic in PVS

- Open the file `pred_basic.pvs` (in Lab1) with PVS and prove all the lemmas.
- Use split, flatten, inst, and skolem (or skeep), and their variants, as appropriate. Do not use the *grind* proof rule.
- Note that most of the lemmas can be discharged automatically with *grind*. However, doing grind will defeat the purpose

Specify a Majority Vote Circuit

- Start a new file in PVS called `majority_vote.pvs`, and enter the relevant specifications for the **relational version** of majority vote.[1]
- Use split, flatten, inst, and skolem (or skeep), and their variants, as appropriate to prove the conjectures.
- You must prove the conjectures `implementation_correctness` and `implementable`. Do not use the *grind* proof rule, but you may use any other proof rules.

[1] Try the functional version on your own. Ensure that you understand the difference.

Specify Telephone Book in PVS

- Start a new file in PVS called `phone.pvs`, and enter the relevant specifications for the telephone book in the WIFT Tutorial: Section 3, A better specification using sets.
- prove all the conjectures without using `grind`.

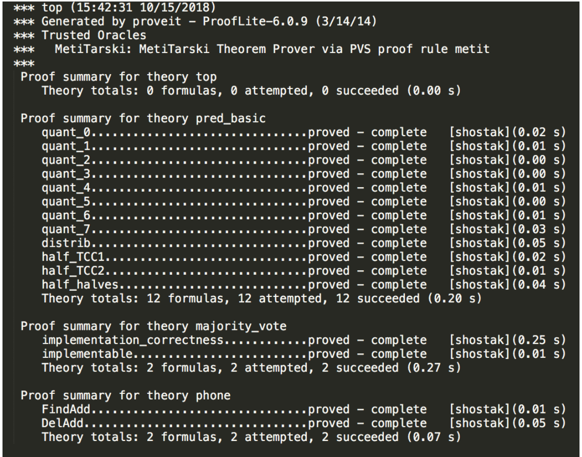
Submit your work 1

- Create a PVS file `top.pvs`

```
% Exercises for Lab5
% proveit --importchain --clean top.pvs
top : THEORY
BEGIN
 IMPORTING pred_basic
 IMPORTING majority_vote
 IMPORTING phone
END top
```

Run Proveit

- In your directory run the following command:
- `proveit --importchain --clean top.pvs`
- You should now see in `top.summary`:



```
*** top (15:42:31 10/15/2018)
*** Generated by proveit - ProofLite-6.0.9 (3/14/14)
*** Trusted Oracles
***   MetiTarski: MetiTarski Theorem Prover via PVS proof rule metit
***
 Proof summary for theory top
    Theory totals: 0 formulas, 0 attempted, 0 succeeded (0.00 s)

 Proof summary for theory pred_basic
    quant_0...............................proved - complete   [shostak](0.02 s)
    quant_1...............................proved - complete   [shostak](0.01 s)
    quant_2...............................proved - complete   [shostak](0.00 s)
    quant_3...............................proved - complete   [shostak](0.00 s)
    quant_4...............................proved - complete   [shostak](0.01 s)
    quant_5...............................proved - complete   [shostak](0.00 s)
    quant_6...............................proved - complete   [shostak](0.01 s)
    quant_7...............................proved - complete   [shostak](0.03 s)
    distrib...............................proved - complete   [shostak](0.05 s)
    half_TCC1.............................proved - complete   [shostak](0.02 s)
    half_TCC2.............................proved - complete   [shostak](0.01 s)
    half_halves...........................proved - complete   [shostak](0.04 s)
    Theory totals: 12 formulas, 12 attempted, 12 succeeded (0.20 s)

 Proof summary for theory majority_vote
    implementation_correctness............proved - complete   [shostak](0.25 s)
    implementable.........................proved - complete   [shostak](0.01 s)
    Theory totals: 2 formulas, 2 attempted, 2 succeeded (0.27 s)

 Proof summary for theory phone
    FindAdd...............................proved - complete   [shostak](0.01 s)
    DelAdd................................proved - complete   [shostak](0.05 s)
    Theory totals: 2 formulas, 2 attempted, 2 succeeded (0.07 s)
```