# Lab6

EECS4312 JSO

October 23, 2018

## Revisions

| Date | Revision | Description |
|---|---|---|
| 12 September 2017 | 1.0 | Initial notes for this document |
| 13 September 2017 | 2.0 | Added Such and Such |

## 1 Precondition

Make sure you are up to date with previous Labs, required self-directed readings, and especially WIFT-95 Tutorials. You should already be skilled in PVS use with propositional logic, predicate logic and set theory applied to the specification of hardware and software systems, and induction.

## 2 Goals

You will learn about specifying functions that are checked for completeness and disjointness via type correctness conditions (TCCs) and also more about specifying recursive functions and validating them with induction. This will be important in our study of the use of function tables for writing precise requirements.

As a byproduct, you will be also be introduced to the fundamental principles behind functional programming languages such as Haskell,

Ocaml and F#. Even OO programming languages such as Eiffel, Java and C# have embraced functional notations and lambda expressions.

# 3 To Do

`top.pvs` lists the theories you must prove.

Start by proving `predicate_thm`:

```
% Exercises for Lab6
% proveit --importchain --clean top.pvs
top : THEORY
BEGIN
   IMPORTING predicate_thm
   IMPORTING alarm
   IMPORTING signum
   IMPORTING stamps
   IMPORTING sqrt2
END top
```

Re-read `sqrt2.spec.pdf` (also provided earlier) for "$\sqrt{2}$ is irrational"proofs. First prove the theorem equationally. You are guided in almost all of the proofs in PVS. The goal is to ensure you are comfortable with the prover.

After you have proved all the theories, execute the following from the command line:

`proveit --importchain --clean top.pvs`

The resulting top.summary should look as shown in the figure on the next page.

```
***
*** top (0:10:55 10/23/2018)
*** 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 predicate_thm
    EA_Thm.............................proved - complete   [shostak](0.01 s)
    EA2_Thm............................proved - complete   [shostak](0.02 s)
    Theory totals: 2 formulas, 2 attempted, 2 succeeded (0.04 s)

 Proof summary for theory alarm
    conjecture1........................proved - complete   [shostak](0.01 s)
    conjecture2........................proved - complete   [shostak](0.00 s)
    Theory totals: 2 formulas, 2 attempted, 2 succeeded (0.01 s)

 Proof summary for theory signum
    sign_TCC1..........................proved - complete   [shostak](0.02 s)
    sign_TCC2..........................proved - complete   [shostak](0.00 s)
    sum_TCC1...........................proved - complete   [shostak](0.01 s)
    sum_TCC2...........................proved - complete   [shostak](0.01 s)
    closed_form........................proved - complete   [shostak](0.13 s)
    sum_of_squares.....................proved - complete   [shostak](0.27 s)
    Theory totals: 6 formulas, 6 attempted, 6 succeeded (0.44 s)

 Proof summary for theory stamps
    stamps.............................proved - complete   [shostak](0.13 s)
    stampf_TCC1........................proved - complete   [shostak](0.01 s)
    stampf_TCC2........................proved - complete   [shostak](0.06 s)
    stampf_TCC3........................proved - complete   [shostak](0.11 s)
    stampf_TCC4........................proved - complete   [shostak](0.05 s)
    stampf_TCC5........................proved - complete   [shostak](0.10 s)
    stampf_TCC6........................proved - complete   [shostak](0.01 s)
    stampf_TCC7........................proved - complete   [shostak](0.00 s)
    stamps_recurs......................proved - complete   [shostak](0.05 s)
    run_stamps_TCC1....................proved - complete   [shostak](0.16 s)
    Theory totals: 10 formulas, 10 attempted, 10 succeeded (0.69 s)

 Proof summary for theory sqrt2
    sqrt4..............................proved - complete   [shostak](0.05 s)
    gcd_conjecture.....................proved - complete   [shostak](0.19 s)
    divides_conjecture.................proved - complete   [shostak](0.02 s)
    conj1..............................proved - complete   [shostak](0.00 s)
    conj2..............................proved - complete   [shostak](0.02 s)
    conj3..............................proved - complete   [shostak](0.04 s)
    conj4..............................proved - complete   [shostak](0.04 s)
    conj5..............................proved - complete   [shostak](0.06 s)
    conj6..............................proved - complete   [shostak](0.08 s)
    conj7..............................proved - complete   [shostak](0.01 s)
    conj8..............................proved - complete   [shostak](0.12 s)
    conj9..............................proved - complete   [shostak](0.03 s)
    PosRational?_TCC1..................proved - complete   [shostak](0.00 s)
    conj10.............................proved - complete   [shostak](0.08 s)
    sqrt2_parta_TCC1...................proved - complete   [shostak](0.00 s)
    sqrt2_parta........................proved - complete   [shostak](0.09 s)
    sqrt2_partb........................proved - complete   [shostak](0.20 s)
    sqrt2_non_rational.................proved - complete   [shostak](0.01 s)
    Theory totals: 18 formulas, 18 attempted, 18 succeeded (1.05 s)

Grand Totals: 38 proofs, 38 attempted, 38 succeeded (2.23 s)
```

Figure 1: top.summary after everything is proved