# Lab7: PVS Function Tables

EECS4312 JSO

October 29, 2018

## Revisions

| Date | Revision | Description |
|---|---|---|
| 12 September 2017 | 1.0 | Initial notes for this document |
| 28 September 2018 | 2.0 | Revise |

## 1 Precondition

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

## 2 Goals

- Using PVS, understand and apply function tables to check completeness and disjointness of specifications

- Use PVS function tables to specify and validate hard real-time systems

# 3 To Do: top.pvs

You must specify and prove three theories as shown in the `top.pvs` file below:

```
% proveit --importchain --clean top.pvs
top : THEORY
BEGIN
   IMPORTING Time
   IMPORTING date
   IMPORTING pressure
   IMPORTING alert
   IMPORTING car_interlock
END top
```

See the `top.summary` file listing all the specification proofs you must complete. Yours might be slightly different for the Car-Interlock (I added a function `car_enter` to help with the function table; you may do it differently).

- *date*: see slides 13 (a partial `date.pvs` is supplied). Use set theory as in the slides. This is to exercise your skill with sets in PVS (higher order logic, where sets are total boolean functions).Prove completeness and disjointness of the specification.

- `pressure.pvs`: See slides 14 for a system specification (where pressure is the **monitored variable** and alarm is the **controlled variable**). Ensure that spec_ft is type correct. Prove an invariant that **validates** the specification. You may use grind (but it is better if your validate the the specification without grind). Import `Time.pvs` theory.

- `alert.pvs`: see slides 14 with **hold-fo**r operator.
  - A Function Table *response* specifies a hold alarm for 1.5 seconds with TR = 0.5 seconds. This function table must be proved complete and disjoint (there are five TCCs, may need grind).
  - Use Case1: Specifies for a given pressure input that $alarm(i)$ holds for $i \in 2 \ldots 5$ and $alarm(6) = FALSE$. Two lemmas

  are used to prove this Use Case. To prove UC1, we need to deal with each of the rows in the *response* function table.

  - Use Case3: Includes UC1 but also but now $alarm(6) = FALSE$.
  - inv_holds safety invariant: anytime pressure is high, there is an alarm. Needs induction.
  - inv2_holds: Whenever pressure is high for 0.5 seconds then alarm is triggered. Needs induction.

- Read car-interlock problem (see PDF). (1) Develop the function table specification and its validation in PVS. (2) Write a requirements document.

See next page for how to submit.

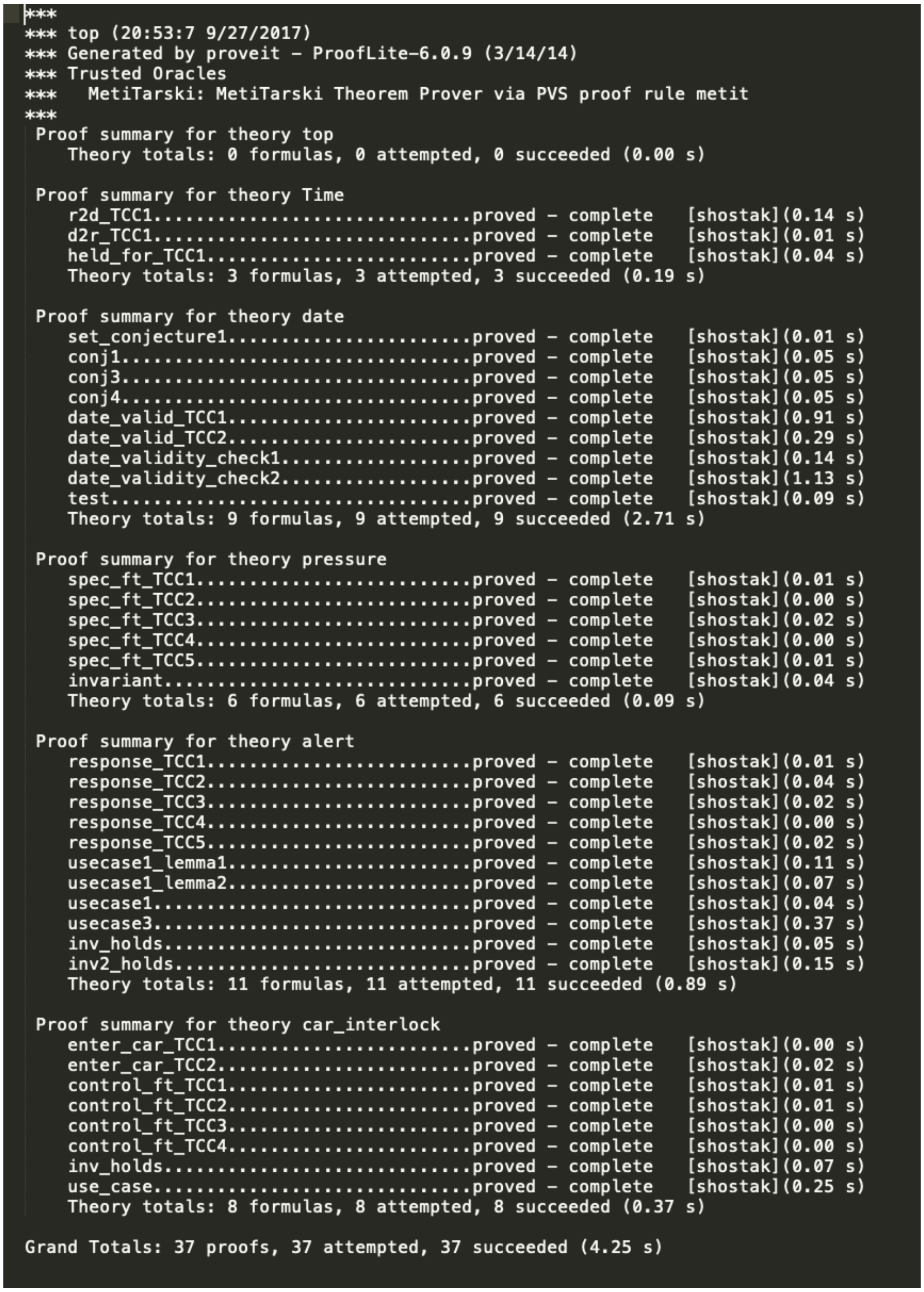
# 4 Submission of this Lab

Create a directory `report` with the following structure:

```
report/
 Car-Interlock-RD.pdf
 pvs/
     Time.prf
     Time.pvs
     alert.prf
     alert.pvs
     car-interlock.prf
     car-interlock.pvs
     date.prf
     date.pvs
     pressure.prf
     pressure.pvs
     top.pvs
     top.summary
```

Then do the following:

```
submit 4312 lab7 report
```



```
***
*** top (20:53:7 9/27/2017)
*** 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 Time
    r2d_TCC1..............................proved - complete   [shostak](0.14 s)
    d2r_TCC1..............................proved - complete   [shostak](0.01 s)
    held_for_TCC1.........................proved - complete   [shostak](0.04 s)
    Theory totals: 3 formulas, 3 attempted, 3 succeeded (0.19 s)

 Proof summary for theory date
    set_conjecture1.......................proved - complete   [shostak](0.01 s)
    conj1.................................proved - complete   [shostak](0.05 s)
    conj3.................................proved - complete   [shostak](0.05 s)
    conj4.................................proved - complete   [shostak](0.05 s)
    date_valid_TCC1.......................proved - complete   [shostak](0.91 s)
    date_valid_TCC2.......................proved - complete   [shostak](0.29 s)
    date_validity_check1..................proved - complete   [shostak](0.14 s)
    date_validity_check2..................proved - complete   [shostak](1.13 s)
    test..................................proved - complete   [shostak](0.09 s)
    Theory totals: 9 formulas, 9 attempted, 9 succeeded (2.71 s)

 Proof summary for theory pressure
    spec_ft_TCC1..........................proved - complete   [shostak](0.01 s)
    spec_ft_TCC2..........................proved - complete   [shostak](0.00 s)
    spec_ft_TCC3..........................proved - complete   [shostak](0.02 s)
    spec_ft_TCC4..........................proved - complete   [shostak](0.00 s)
    spec_ft_TCC5..........................proved - complete   [shostak](0.01 s)
    invariant.............................proved - complete   [shostak](0.04 s)
    Theory totals: 6 formulas, 6 attempted, 6 succeeded (0.09 s)

 Proof summary for theory alert
    response_TCC1.........................proved - complete   [shostak](0.01 s)
    response_TCC2.........................proved - complete   [shostak](0.04 s)
    response_TCC3.........................proved - complete   [shostak](0.02 s)
    response_TCC4.........................proved - complete   [shostak](0.00 s)
    response_TCC5.........................proved - complete   [shostak](0.02 s)
    usecase1_lemma1.......................proved - complete   [shostak](0.11 s)
    usecase1_lemma2.......................proved - complete   [shostak](0.07 s)
    usecase1..............................proved - complete   [shostak](0.04 s)
    usecase3..............................proved - complete   [shostak](0.37 s)
    inv_holds.............................proved - complete   [shostak](0.05 s)
    inv2_holds............................proved - complete   [shostak](0.15 s)
    Theory totals: 11 formulas, 11 attempted, 11 succeeded (0.89 s)

 Proof summary for theory car_interlock
    enter_car_TCC1........................proved - complete   [shostak](0.00 s)
    enter_car_TCC2........................proved - complete   [shostak](0.02 s)
    control_ft_TCC1.......................proved - complete   [shostak](0.01 s)
    control_ft_TCC2.......................proved - complete   [shostak](0.01 s)
    control_ft_TCC3.......................proved - complete   [shostak](0.00 s)
    control_ft_TCC4.......................proved - complete   [shostak](0.00 s)
    inv_holds.............................proved - complete   [shostak](0.07 s)
    use_case..............................proved - complete   [shostak](0.25 s)
    Theory totals: 8 formulas, 8 attempted, 8 succeeded (0.37 s)

Grand Totals: 37 proofs, 37 attempted, 37 succeeded (4.25 s)
```

Figure 1: top.summary after everything is proved