CS 511 – Fall 2020 Semester

CS 511 Official Website: Formal Methods for High-Assurance Software Engineering

CS 511 Piazza Website: for all communications, announcements, and extra material

Instructor: Assaf Kfoury

Lectures: Tue, Thur, 12:30-1:45 pm
Tutorial Labs: Wedn, 2:30-3:20 pm

9 September 2020

Addendum 03

Announcements:

Homework Assignment # 01:

- Posted on Friday, Sept 4.
- Due on Friday, Sept 11, by 11:59 pm.

Homework Assignment # 02:

- Posted on Friday, Sept 11.
- Due on Friday, Sept 18, by 11:59 pm.

(Partial) Lecture Notes:
From Compactness to Completeness [2020-09-07.fCtC],
posted on *Piazza* under *Resources*.

For more examples of *natural-deduction proofs*,
besides those in the book (sometimes using slightly
different conventions) and those in Handout 02, see:

- page 43 (marked 63) in [2020-09-07.fCtC],
- page 47 (marked 67) in [2020-09-07.fCtC], Example 83.

Scripts for Z3 and Z3Py used in yesterday's tutorial are posted

Request:

- Try to ask your questions on Piazza so that they are **visible** to everyone.
- There is no problem if you choose to ask them anonymously.
- I always prefer my answers to be **visible** to everyone.

Some Acronyms and Abbreviations:

SAT = propositional/Boolean **sat**isfiability

SAT solver = automated tool that decides whether a propositional wff is satisfiable

SMT = **s**atisfiability **m**odulo a first-order **t**heory

SMT solver = automated tool that decides whether a wff from a first-order theory is satisfiable

ATP = **a**utomated **t**heorem **p**rover

ITP = **i**nteractive **t**heorem **p**rover
(sometimes called **IPA** = **i**nteractive **p**roof **a**ssistant)

CF = **c**ounterexample/**c**ountermodel **f**inder
(sometimes called **CG** = **c**ounterexample/**c**ountermodel **g**enerator)

Examples of Automated Tools
– hopefully we will use them with interesting CS problems this semester:

- **Z3** is a SAT/SMT solver
- **Prover9** is an ATP (perhaps this semester)
- **Vampire** is an ATP (perhaps this semester)
- **Mace4** is a CF (perhaps this semester)

Other Examples of Automated Tools
– not used this semester:

- **Coq** is an ITP / IPA
- **Isabelle/HOL** is an ITP / IPA
- **Nitpick** is a CF for Isabelle
- and many other

But SAT/SMT solvers, ATP's, ITP's, IPA's, CF's, and CG's, are not the only logic-based automated tools. Notably missing from the preceding list are many **model-checkers**.

Correction:

On Tuesday, I showed two scripts, `majority.smt2` and `majority.py`, both intended to show to show $\varphi \Leftrightarrow \psi$ where φ is the DNF of the majority function and ψ is the CNF of the majority function.

To show that φ and ψ are equivalent, it is not enough to verify that $\varphi \Leftrightarrow \psi$ is **satisfiable**. We must verify instead that $\neg(\varphi \Leftrightarrow \psi)$ is **unsatisfiable**.

The corrected scripts are posted.

(THIS PAGE INTENTIONALLY LEFT BLANK)