CS 499 – Mechanized Reasoning about Programs

Project Assignments 2 to 4

Due dates: 11/16, 11/30, 12/07

Abstract

The goal of the project is to implement a certified compiler for the **While** language. The target language is a small abtract machine.

1 The Abstract Machine

The first step of PA2 is to formalize the abstract machine **AM** of Semantics with Applications described in Chapter 4:

- *storage* as well as *states* should be formalized as total functions,
- the semantics of **AM** should be formalized as an inductively defined proposition (relation),
- examples 4.1 and 4.2 should be used as tests for your formalization.

It is recommended to request a feedback on your formalization before starting the second part.

The second step of PA2 is to prove some properties of this semantics: the properties stated in Exercise 4.4, Exercise 4.5 and Exercise 4.6.

PA2 is due on November 16, 2016.

2 Specification of the Translation

The first part of PA3 is to formalize the compilation from **While** to **AM**. Examples 4.10 and 4.12 should be used as tests for your translation functions.

It is recommended to request a feedback on your formalization before starting the second part.

The second part of PA3 is to prove Lemma 4.18 and Lemma 4.19.

PA3 is due on November 30, 2016

3 Correctness

It is not possible to define $\mathcal{S}_{\text{ns}}$ and $\mathcal{S}_{\text{am}}$ as functions in Coq. It is however possible to define them as relations. The statement and proof of Theorem 4.20 is a bonus question.

The goal of PA4 is to prove Lemma 4.21 and Lemma 4.22.

PA4 is due on December 7, 2016