Lab 4 - Deductive Verification

Welcome to lab 4! In this lab you will learn how to perform deductive software verification of C programs with the Frama-C toolkit.

Requirements

In order to work on this lab assignment you need to have a working Frama-C installation. You can follow the installation instructions here.

If you are working on a Mac, there seems to be a problem with GTK (the GUI framework Frama-C uses). In some cases it helps to install the previous version of Frama-C. To do so just use

```
opam install frama-c.25.0
```

instead of

```
opam install frama-c
```

Apparently it may also help to install the new GUI called *Ivette*. Instructions for installing *Ivette* are given on the command line once you have finished installing Frama-C. **We will not use Ivette in this lab, so you do not need to install it if the normal Frama-C installation works**.

To test if your installation was successful issue the following on a command line:

```
frama-c-gui
```

This should open the GUI for Frama-C.

If you cannot/don't want to install Frama-C, you can use the provided VM, which can be downloaded here. The Linux VM has Frama-C installed. In `/docs/instructions_VM.txt` (in template), you will find brief instructions on how to set up the VM.

Template

You can download the template from Studium.

Goal

This lab is a bit different then the previous ones. In the template, there is a document called **frama_c_tutorial.pdf** under the `/docs` directory. This tutorial will walk you through some of the most important aspects of working with function contracts and using Frama-C to prove them correct. You are supposed to work through this document, and solve the exercises at the end of each section.

In the template there is a folder called `/exercises` that has stub implementations for each exercise.

Resources

The main resource for this lab is the provided tutorial. However, you may find these additional documents helpful. All of them are provided in the `/docs` directory in the lab template.

- Frama-C User Manual
- ACSL Language Specification
- Introduction to C program proof with Frama-C and its WP plugin