Developing an Interactive, Web-Based Tutorial for an Intermediate Verification Language

Mathias Birrer
matbirre@student.ethz.ch

Supervised by Malte Schwerhoff

21.03.2015

1 Motivation

The Viper[1] verification infrastructure is built for permission based reasoning and provides an intermediate verification language (IVL) called Silver, that natively supports an expressive permission model and a set of carefully chosen language constructs that enables an encoding of a wide range of higher-level programming and specification features. The Viper verification infrastructure includes two back-end verifiers called Silicon and Carbon.

Since only a technical report[2] of Silver exists, the effort needed to get started with the Silver IVL is very high. A tutorial which explains the basic features and demonstrates how to encode features from high-level languages into Silver would make it more easily accessible to interested people.

In an earlier Bachelor's thesis, a web interface called Tuwin, which allows to use various verification tools, has been developed[3]. Such a web-based access simplifies the use of verification tools a lot.

With the existing web-based access to verification tools, we can create an interactive tutorial for the Silver IVL. Interactive means that the reader of the tutorial is able to write and try some examples right on the tutorial page, which leads to a more hands-on introduction to Silver.

The following picture shows a possible design of the interactive tutorial, where the text floats around a code input box.

[1] http://www.pm.inf.ethz.ch/research/viper

[2] http://pm.inf.ethz.ch/publications/getpdf.php?bibname=Own&id=JKMNSS14.pdf

[3] http://www.pm.inf.ethz.ch/education/theses/student_docs/Roland_Meyer/Roland_Meyer_BA_report

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla

2. Lorem ipsum dolor sit amet

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

```
class Math {
    method ISqrt(n: int) returns (res: int)
        requires 0 <= n;
        ensures res * res <= n && n < (res+1) * (res+1);
    {
        res := 0;
        while ((res + 1) * (res + 1) <= n)
            invariant res * res <= n;
        {
            res := res + 1;
        }
    }
}
```

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla

Figure 1: Possible layout for the interactive tutorial

2 Core Goals

The core goal of this Bachelor's thesis is to develop an interactive tutorial for the Silver IVL. The following points clarify the tasks related to the core goal:

- Create an interactive tutorial for the Silver IVL. The tutorial is a combination of a normal tutorial that explains the features of Silver and an online verification tool, with which the reader can try examples themselves.
- The tutorial should address an audience that has some general experience in software verification, but not necessarily in permission-based reasoning, and is interested in learning the advantages of the Silver IVL.
- The tutorial should be rich in examples and tasks the reader can try themselves with the online verification tool.
- The tool used for online verification has very high latency in its current version. The performance of this tool has to be improved such that the response time becomes acceptable for an interactive tutorial.

3 Schedule

The following items summarize the tasks this thesis includes. The percentage should offer a rough estimation of how much time is planned to complete them:

- Familiarize with Silver (5%)
- Familiarize with the Scala language and the code of the Viper tools (10%)
- Write tutorial content (30%)
- Update Tuwin libraries (10%)
- Make Silicon and Carbon available through the web interface (10%)
- Further development of Tuwin, e.g. reduce response time and improve user interface (15%)
- Implement interactive tutorial (10%)
- Write report (10%)

4 Extensions

If time permits, the following extensions could be addressed:

Cover additional Silver features in the tutorial
The Silver language offers some features such as magic wands, quantified permissions and obligations, which are still under development. One or more of those could be covered in the tutorial as an extension.

Simplify process of adding tool support
The current process to add a new verification tool to the Tuwin web interface is not easy, and also not optimal from a security point of view. Both issues could be addressed as an extension.

Improve online code editor
The used code editor is very flexible and can be adapted in many ways. Another possible extension is to implement nice-to-have features such as autocompletion or code folding.