Lightweight Support for Magic Wands in an Automatic Verifier (Artifact)

Malte Schwerhoff and Alexander J. Summers

ETH Zürich, Switzerland
{malte.schwerhoff,alexander.summers}@inf.ethz.ch

Abstract

This artifact is based on Silicon, which is an automatic verification tool for programs written in the Silver Intermediate Verification Language. Silver is designed to natively support permission-based reasoning, in the style of separation logic and similar approaches. Our extension of Silicon provides support for specification and verification of programs using the *magic wand* operator, which can be used to represent ways to exchange views on the program state, or to represent partial versions of data structures. Our implementation is a backwards-compatible extension of the basic tool, and is provided along with a test suite of examples and regressions in a VirtualBox image. Instructions for running our tool on these (and user-defined) examples are provided in the image, to allow users to experiment with the verifier.

1998 ACM Subject Classification F.3.1 Specifying and Verifying and Reasoning about Programs

Keywords and phrases Magic Wand, Software Verification, Automatic Verifiers, Separation Logic, Implicit Dynamic Frames

Digital Object Identifier 10.4230/DARTS.1.1.10

Related Article Malte Schwerhoff and Alexander J. Summers, "Lightweight Support for Magic Wands in an Automatic Verifier", in Proceedings of the 29th European Conference on Object-Oriented Programming (ECOOP 2015), LIPIcs, Vol. 37, pp. 614–638, 2015.
http://dx.doi.org/10.4230/LIPIcs.ECOOP.2015.614

Related Conference 29th European Conference on Object-Oriented Programming (ECOOP 2015), July 5–10, 2015, Prague, Czech Republic

1 Scope

The artifact allows repeatability of the verification results documented in the paper, as well as providing users with the opportunity to modify our test cases or experiment with their own, in order to evaluate the usability of the magic wand support detailed in our paper. Simple scripts are provided to allow the examples to be run directly on the command-line, along with detailed instructions.

2 Content

The artifact package includes:

- a binary of Silicon with support for magic wands
- a binary of Z3 4.3.2, the SMT solver Silicon uses
- detailed instructions for running Silicon, and suggestions how to modify the examples mentioned in our paper, e.g. to provoke a verification failure

To simplify the use of Silicon we provide a VirtualBox disk image containing a lightweight Linux distribution fully configured for running Silicon. The image contains SLiTaZ 4.0 (`http://www.slitaz.org`), a small Linux distribution with a graphical user interface, a few text editors (Leafpad and others), Oracle JVM 1.7.0, and of course binaries of Silicon and Z3. Log in using `silicon:silicon` (or, if need be, `root:root`).

3 Getting the artifact

The artifact endorsed by the Artifact Evaluation Committee is available free of charge on the Dagstuhl Research Online Publication Server (DROPS). The latest version of our implementation is available via our bitbucket repositories at: `https://bitbucket.org/viperproject/silicon` and detailed information is available at `http://www.pm.inf.ethz.ch/research/viper.html`.

4 Tested platforms

We used Oracle VirtualBox 4.3.20 on Windows 7 x64 to boot the VirtualBox image. The host computer was equipped with 8 GB RAM, but since the Linux installation contained in the image is relatively small and optimised for computers with limited resources, the image should also be useable on computers with less RAM. Artefact reviewers successfully used the artefact on Mac OS X, versions 10.10.2 and 10.10.3, and on Linux 2.6.32 (distribution unknown).

5 License

Silicon and all files of its source code are licensed under the Mozilla Public License Version 2.0 (`http://www.mozilla.org/MPL/2.0/`), with the following *exceptions*:

- Files found in the following *source* (e.g. when browsing Silicon's sources, rev. d0eef64, on Bitbucket) directories (and their sub-directories) in the Silicon hierarchy, which are licensed under Public Domain (see `http://creativecommons.org/publicdomain/zero/1.0/`):
  - `docs/licenses`
  - `project`
  - `src/test/resources`
  - `utils`
- Files found in the source directory `src/main/resources/dafny_axioms` (and its sub-directories), which are licensed under Microsoft Public License (Ms-PL) (see `http://dafny.codeplex.com/license`).
- All software provided in the VirtualBox other than Silicon, is provided under its own licences. For example, the included version of Z3 is also provided under the Microsoft Public License (Ms-PL).

6 MD5 sum of the artifact

48b95a24e7cf17709871947c5d6b199b

7 Size of the artifact

349 MB

Acknowledgements. The authors were funded by the Hasler Foundation. We are very grateful to Peter Müller, Ioannis T. Kassios, Uri Juhasz and John Boyland for extensive feedback on earlier versions of this work.