Compositional Symbolic Execution for Correctness and Incorrectness Reasoning (Artifact)

Andreas Lööw
Imperial College London, UK

Daniele Nantes-Sobrinho
Imperial College London, UK

Sacha-Élie Ayoun
Imperial College London, UK

Caroline Cronjäger
Ruhr-Universität Bochum, Germany

Nat Karmios
Imperial College London, UK

Petar Maksimović
Imperial College London, UK
Runtime Verification Inc., Chicago, IL, USA

Philippa Gardner
Imperial College London, UK

Abstract

This artifact is a companion to the paper "Compositional Symbolic Execution for Correctness and Incorrectness Reasoning". It contains the source code of the Gillian compositional symbolic execution (CSE) platform, in which we added the incorrectness reasoning capabilities, and the benchmarks used in the evaluation of the paper. It also contains a Haskell demonstrator CSE engine that directly implements the CSE engine inference rules presented in the paper.

2012 ACM Subject Classification Theory of computation → Program verification; Theory of computation → Program analysis; Theory of computation → Separation logic; Theory of computation → Automated reasoning

Keywords and phrases separation logic, incorrectness logic, symbolic execution, bi-abduction

Digital Object Identifier 10.4230/DARTS.10.2.13

Funding This work was supported by the EPSRC Fellowship "VetSpec: Verified Trustworthy Software Specification" (EP/R034567/1).

Acknowledgements We would like José Fragoso Santos for producing the original version of Gillian. We would also like to thank the anonymous reviewers for their comments.

Related Article Andreas Lööw, Daniele Nantes-Sobrinho, Sacha-Élie Ayoun, Caroline Cronjäger, Petar Maksimović, and Philippa Gardner, "Compositional Symbolic Execution for Correctness and Incorrectness Reasoning", in 38th European Conference on Object-Oriented Programming (ECOOP 2024), LIPIcs, Vol. 313, pp. 25:1–25:28, 2024.
https://doi.org/10.4230/LIPIcs.ECOOP.2024.25

Related Conference 38th European Conference on Object-Oriented Programming (ECOOP 2024), September 16–20, 2024, Vienna, Austria

Evaluation Policy The artifact has been evaluated as described in the ECOOP 2024 Call for Artifacts and the ACM Artifact Review and Badging Policy.

Dagstuhl Artifacts Series
Schloss Dagstuhl – Leibniz-Zentrum für Informatik,
Dagstuhl Publishing, Germany

1 Scope

The paper makes the following claims:

- We have extended the Gillian platform with support for under-approximate (UX) reasoning and UX bi-abduction.
- These modifications have not broken backward compatibility, and the existing analyses implemented before in Gillian remain unaffected.
- Additionally, we have developed a prototype Haskell implementation of the compositional symbolic execution (CSE) engine described in the paper, to ensure that the inference-rules description of the engine in the paper is directly implementable.

These caims are backed by the artifact, which contains the implementation of Gillian enhanced with support of UX reasoning and bi-abduction, together with scripts to reproduce the benchmarks presented in the paper, and benchmarks presented in previous work. It also contains the Haskell implementation which can be inspected.

2 Content

The artifact package includes:

- A README file with instructions on how to install and run the artifact.
- A VirtualBox image containing the Gillian code and Haskell implementation.

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). In addition, the artifact is also available at: `https://zenodo.org/records/12675498`.

4 Tested platforms

We have tested the VM on a machine with the following configuration: MacbookPro 2019, 2.3GHz 8-Core Intel Core i9, 16GB 2667 MHz DDR4, MacoOS Sonoma 14.5. We expect the VM to work on any machine able to allocate 2CPUs and 8GB of RAM to the VM.

5 License

The artifact is available under license Creative Commons Attribution 4.0 International

6 MD5 sum of the artifact

0b18868dfa3cdeeebadefa7fd3266057

7 Size of the artifact

10.56 GiB