

Verifying Lock-Free Search Structure Templates (Artifact)

Nisarg Patel 

New York University, NY, USA

Dennis Shasha 

New York University, NY, USA

Thomas Wies 

New York University, NY, USA

Abstract

We present and verify template algorithms for lock-free concurrent search structures that cover a broad range of existing implementations based on lists and skiplists. Our linearizability proofs are fully mechanized in the concurrent separation logic Iris. The proofs are modular and cover the broader design space of the underlying algorithms by parameterizing the verification over aspects such as the low-level representation of nodes and the style of

data structure maintenance. As a further technical contribution, we present a mechanization of a recently proposed method for reasoning about future-dependent linearization points using hindsight arguments. The mechanization builds on Iris' support for prophecy reasoning and user-defined ghost resources. We demonstrate that the method can help to reduce the proof effort compared to direct prophecy-based proofs.

2012 ACM Subject Classification Theory of computation → Logic and verification; Theory of computation → Separation logic; Theory of computation → Shared memory algorithms

Keywords and phrases skiplists, lock-free, separation logic, linearizability, future-dependent linearization points, hindsight reasoning

Digital Object Identifier 10.4230/DARTS.10.2.15

Funding This work is funded in parts by NYU Wireless and by the United States National Science Foundation under grants CCF-2304758, 1840761, 2304758, and 25-74100-F1202. Further funding came from an Amazon Research Award Fall 2021. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views of Amazon.

Related Article Nisarg Patel, Dennis Shasha, and Thomas Wies, “Verifying Lock-Free Search Structure Templates”, in 38th European Conference on Object-Oriented Programming (ECOOP 2024), LIPIcs, Vol. 313, pp. 30:1–30:28, 2024.

<https://doi.org/10.4230/LIPIcs.ECOOP.2024.30>

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.

1 Scope

The artifact contains the Coq files for: (i) formalizing the hindsight framework in Iris; and (ii) verifying the skiplist template presented in the related paper. The artifact contains scripts to generate Table 1 from Section 6 of the related paper.

2 Content

The artifact package includes:

 © Nisarg Patel, Dennis Shasha, and Thomas Wies; licensed under Creative Commons License CC-BY 4.0
Dagstuhl Artifacts Series, Vol. 10, Issue 2, Artifact No. 15, pp. 15:1–15:2
 DAGSTUHL ARTIFACTS SERIES
Dagstuhl Artifacts Series
Schloss Dagstuhl – Leibniz-Zentrum für Informatik,
Dagstuhl Publishing, Germany



15:2 Verifying Lock-Free Search Structure Templates (Artifact)

- `lockfree-templates.ova` : an Ubuntu 22.04 VM (with GUI) containing the Coq environment and the files relevant to the development.
- `docker-lockfree-templates.tar` : a Docker image for Apple M-series chips containing the same files as above.
- `ecoop24_artifact.zip` : the artifact files relevant to the development for easy access.
- `ECOOP_AE_Submission_104.md` : contains additional detail on how to run the artifact, reuse, etc.
- `summary_of_revisions.txt` : contains a summary of changes in the revised submission for artifact evaluation.

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 on Zenodo at: <https://zenodo.org/doi/10.5281/zenodo.10548260>.

4 Tested platforms

The artifact contains the files in two forms: (i) an Ubuntu VM built and tested on Linux (Fedora); and (ii) a Docker image built and tested on Apple M1 computer. Please see the file `ECOOP_AE_Submission_104.md` in the artifact for more details.

5 License

Please see file `ecoop24_artifact/LICENSE` for license details.

6 MD5 sum of the artifact

`c6be28b5f055d3388227d32bd080121c`

7 Size of the artifact

11.34 GB