Owicki-Gries Reasoning for C11 RAR (Artifact)

Sadegh Dalvandi
University of Surrey, United Kingdom
m.dalvandi@surrey.ac.uk

Simon Doherty
University of Sheffield, United Kingdom
s.doherty@sheffield.ac.uk

Brijesh Dongol
University of Surrey, United Kingdom
b.dongol@surrey.ac.uk

Heike Wehrheim
Paderborn University, Germany
wehrheim@upb.de

Abstract

The paper "Owicki-Gries Reasoning for C11 RAR" introduces a new proof calculus for the C11 RAR memory model that allows Owicki-Gries proof rules for compound statements, including non-interference, to remain unchanged. The proof method features novel assertions specifying thread-specific views on the state of programs. This is combined with a set of Hoare logic rules that describe how these assertions are affected by atomic program steps. The artifact includes the Isabelle formalisation of the proof method introduced in the paper. It also contains the formalisation and proof of all case studies presented in the paper. All of the theorems are accompanied with their respective proofs.

2012 ACM Subject Classification Theory of computation → Logic and verification; Theory of computation → Hoare logic; Theory of computation → Concurrency; Theory of computation → Operational semantics; Theory of computation → Program reasoning

Keywords and phrases C11, Verification, Hoare logic, Owicki-Gries, Isabelle

Digital Object Identifier 10.4230/DARTS.6.2.15

Funding *Sadegh Dalvandi*: Supported by EPSRC Grant EP/R032556/1.
Simon Doherty: Supported by EPSRC Grant EP/R032351/1.
Brijesh Dongol: Supported by EPSRC Grant EP/R032556/1.
Heike Wehrheim: Supported by DFG grant WE 2290/12-1.

Related Article Sadegh Dalvandi, Simon Doherty, Brijesh Dongol, and Heike Wehrheim, "Owicki-Gries Reasoning for C11 RAR", in 34th European Conference on Object-Oriented Programming (ECOOP 2020), LIPIcs, Vol. 166, pp. 11:1–11:26, 2020. https://doi.org/10.4230/LIPIcs.ECOOP.2020.11

Related Conference 34th European Conference on Object-Oriented Programming (ECOOP 2020), November 15–17, 2020, Berlin, Germany (Virtual Conference)

1 Scope

The artifact is a set of Isabelle[1] theories formalising the proof method introduced in the paper "*Owicki-Gries Reasoning for C11 RAR*". More precisely, it includes the formalisation of an operational semantics for the RAR fragment of C11, formalisation of the novel assertions introduced in the paper, together with the mechanised proof of all proof rules and case studies provided in the paper.

[1] https://isabelle.in.tum.de/

2 Content

The artifact package includes a number of Isabelle theories and a more detailed description:

- **OpSem.thy** includes the formalisation of the proof method together with all the rules and their proof.
- **LB.thy** includes an encoding of the load buffering litmus test, its proof outline and the associated proof (Figure 8, Section 5.3 of the paper).
- **MP.thy** includes an encoding of the message passing litmus test, its proof outline and the associated proof (Figure 3, Section 5.4 of the paper).
- **RRC_2T.thy** includes an encoding of a two threaded version of the read-read coherence litmus test, its proof outline and the associated proof (Figure 9, Section 5.5 of the paper).
- **RRC_3T.thy** includes an encoding of a three threaded version of the read-read coherence litmus test, its proof outline and the associated proof (not included int the paper).
- **RRC.thy** includes an encoding of a four threaded version of the read-read coherence litmus test, its proof outline and the associated proof (Figure 10, Section 5.5 of the paper).
- **Petersons.thy** includes an encoding of the Peterson's mutual exclusion algorithm case study presented in Section 6 of the paper together with its proof outline and the associated proof.
- **ReadMe.pdf** which includes a documentation for the artifact and also provides details on how the artifact is related to the formalisation and proof provided in the paper.
- **license.txt** which includes the license notice of the artifact.

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://doi.org/10.6084/m9.figshare.12424859`.

4 Tested platforms

Since the artifact is the formalisation of the proof method in Isabelle/HOL, no installation or compilation for the artifact is required. No external library or prover other than those provided by the standard distribution of Isabelle/HOL is used. The theories have been checked against both Isabelle2019/HOL and (the recently released) Isabelle2020/HOL, and they go through without any problem.

5 License

The artifact is available under the 3-Clause BSD License (BSD-3-Clause).

6 MD5 sum of the artifact

2af93230c931e280e342352f5c7ce83e

7 Size of the artifact

209,939 bytes