Hyper Hoare Logic: (Dis-)Proving Program Hyperproperties (Artifact)

Overview

This document describes the artifact submitted in support of the PLDI 2024 submission "Hyper Hoare Logic: (Dis-)Proving Program Hyperproperties", which consists of an Isabelle/HOL mechanization that fully supports the formal claims made in the paper.

Get Started

The artifact is a VirtualBox VM image that contains Isabelle 2023, and our Isabelle/HOL formalization. To run it, simply import it into an up-to-date version of VirtualBox (we tested with version 7.0). It uses 8GB of RAM and two logical cores by default; if these values are too high for your system, feel free to adjust the number of cores, but the VM may not work correctly with less than 8GB of RAM. The username is "vboxuser" and the password "pldi24".

To get started, we recommend making sure that all the files are successfully verified by Isabelle.

Our mechanization is located in ~/artifact/mechanization, and it contains the following 10 Isabelle files (we describe the contents of each file in the "Step by Step" part):

- PaperResults.thy
- Language.thy
- Logic.thy
- ProgramHyperproperties.thy
- SyntacticAssertions.thy
- Loops.thy
- Expressivity.thy
- Compositionality.thy
- ExamplesCompositionality.thy
- TotalLogic.thy

a. Using Isabelle's CLI

One can check that Isabelle successfully verifies all 10 files using the Isabelle command line interface (located at *~/Isabelle2023/bin/isabelle*, accessible in the terminal via the alias *isabelle*) with the command *"isabelle build -c -d. -l HyperHoareLogic"* (this command tells Isabelle to build the *HyperHoareLogic* session, which is defined in the *ROOT* file), run from the folder ~/artifact/mechanization.

This can be achieved with the following command:

```
> cd ~/artifact/mechanization
> isabelle build -c -d. -l HyperHoareLogic
```

Expected output:

The final lines of the output should look like the following:

```
…
Session Unsorted/HyperHoareLogic
  /home/vboxuser/artifact/mechanization/Compositionality.thy
  /home/vboxuser/artifact/mechanization/ExamplesCompositionality.thy
  /home/vboxuser/artifact/mechanization/Expressivity.thy
  /home/vboxuser/artifact/mechanization/Language.thy
  /home/vboxuser/artifact/mechanization/Logic.thy
  /home/vboxuser/artifact/mechanization/Loops.thy
  /home/vboxuser/artifact/mechanization/PaperResults.thy
  /home/vboxuser/artifact/mechanization/ProgramHyperproperties.thy
  /home/vboxuser/artifact/mechanization/SyntacticAssertions.thy
  /home/vboxuser/artifact/mechanization/TotalLogic.thy
Cleaned HyperHoareLogic
Running HyperHoareLogic …
Finished HyperHoareLogic (0:01:22 elapsed time, 0:02:08 cpu time, factor 1.55)
0:01:30 elapsed time, 0:02:08 cpu time, factor 1.42
```

This output indicates that Isabelle successfully verified the 10 files in 1 minute and 22 seconds (it might take a bit longer depending on your configuration). A different output might indicate a problem.

b. Using Isabelle's GUI

Isabelle's graphical user interface, located at *~/Isabelle2023/Isabelle2023* and at the terminal alias *isabelle_gui,* can also be used to ensure that Isabelle can verify all files. To verify that a file is successfully verified:

1. Open the file (File > Open…). We recommend opening the file *PaperResults.thy*, which contains all the claims made in the paper as well as explanations, and imports all other files.
2. Open the Theories panel (Plugins > Isabelle > Theories panel). It should be visible on the right of the window.
3. Activate "continuous checking" by ticking the box at the top of the Theories panel, if it is not already activated.
4. Put the cursor at the end of the file.

The verification status can be seen on the right of the editor, next to the scrollbar:

- Pink indicates a part that has not been verified yet.
- Purple indicates ongoing verification.
- Clear or orange indicates successful verification. Orange indicates a warning (warnings do not indicate invalid proofs, but correct proofs that can be optimized).
- Red indicates an error (this should *not* happen).

Moreover, the “Theories” panel shows the verification status of all files that are imported by the file we opened.

To jump to the definition of a term, click on it while holding the Control key.

Step by Step Instructions

To check that the claims made in the paper are supported by our Isabelle formalization, we recommend to open side by side the PDF of the paper (located at *~/artifact/paper.pdf*) and the Isabelle file *PaperResults.thy* (located at *~/artifact/mechanization/PaperResults.thy*) using the Isabelle GUI (see how to in the *Getting Started Guide*). The file *PaperResults.thy* contains all the formal results presented in the paper, in the same order as the paper, and contains explanations of how the formalization relates to the paper. You can then follow the paper, and check that every formal claim in the paper as a counterpart in the Isabelle formalization. The file *PaperResults.thy* also contains the formal results presented in the appendix of the paper (located at *~/artifact/appendix.pdf)*.

Structure of the mechanization

We briefly describe the structure of the mechanization here. However, we highly recommend the file *PaperResults.thy* as the entry point to the formalization (and using ctrl+click on Isabelle terms to navigate the formalization).

PaperResults.thy
This file contains all the formal results presented in the paper, in the same order as the paper. It is meant to be the entry point from the paper into the rest of the formalization.

Language.thy
In this file, we formalize results from section 3:

- Program states (definition 1)
- Programming language (definition 1)
- Big-step semantics (figure 2)
- Extended states (definition 2)
- Extended semantics (definition 4) and some useful properties (lemma 1)›

Logic.thy

This file contains technical results from section 3:

- Hyper-assertions (definition 3)
- Hyper-triples (definition 5)
- Core rules of Hyper Hoare Logic (figure 3)
- Soundness of the core rules (theorem 1)
- Completeness of the core rules (theorem 2)
- Ability to disprove hyper-triples (theorem 4)

ProgramHyperproperties.thy
In this file, we define program hyperproperties (definition 8), and prove theorem 3.

SyntacticAssertions.thy
This file contains the technical results from section 4:

- Definition of syntactic hyper-assertions
- Proof of the syntactic rules (figure 4)

Loops.thy
This file contains the technical results from section 5: It contains the proofs of the loop rules shown in figure 6.

Expressivity.thy
In this file, we prove most results of appendix C: the judgments of many Hoare logics can be encoded as hyper-triples. Hyper-triples subsume many other triples, as well as example 3.

Compositionality.thy
In this file, we prove the soundness of all compositionality rules presented in appendix D (figure 11).

ExamplesCompositionality.thy
In this file, we prove compositionality examples from Appendix D.2.

TotalLogic.thy
This file contains the technical results of appendix E (termination-based reasoning):

- Definition of total hyper-triples (definition 24)
- Proof of the rules Frame and WhileSyncTot

Reusing the Isabelle mechanization outside the VM

To reuse the artifact outside the VM, you need to install the proof assistant Isabelle. Isabelle can be easily downloaded and installed from https://isabelle.in.tum.de/installation.html. It can be installed on Linux, Windows, MacOS, and it is also available as a Docker image. In this document, we assume that Isabelle has been installed at the path ~/Isabelle2023.

Note that we have only tested our mechanization with the version 2023 of Isabelle. Some proofs might fail with earlier versions.