Artifact for the paper “Fractional Resources in Unbounded Separation Logic”

Overview

This is the artifact for the OOPSLA 2022 paper “Fractional Resources in Unbounded Separation Logic”, which contains an Isabelle/HOL formalisation (in the form of a parametric theory) that proves the technical claims from the paper.

We describe below how to get started, namely how to install Isabelle/HOL and ensure that all files are successfully verified by Isabelle. We then describe the structure of the formalisation, and finally provide a correspondence between the claims in the paper and the results in the formalisation.

Getting started

To get started, we recommend the following three steps: (1) Install Isabelle/HOL 2021-1, (2) make sure that all the files are successfully verified by Isabelle, (3) verify the absence of unjustified assumptions.

(1) Install Isabelle/HOL 2021-1

The proof assistant Isabelle can be easily downloaded and installed from https://isabelle.in.tum.de/installation.html. It can be installed on Linux, Windows 10, MacOS, and it is also available as a Docker image. Later in this document, we assume that Isabelle has been installed at the path */path/to/Isabelle2021-1*.

Note that we have only tested our formalisation with the version 2021-1. Some proofs might fail with earlier versions.

(2) Make sure that all files are successfully verified by Isabelle

Our formalisation contains the following 6 Isabelle files:

- AutomaticVerifiers.thy
- Combinability.thy
- FixedPoint.thy
- Properties.thy
- UnboundedLogic.thy
- WandProperties.thy

a. Using Isabelle’s CLI

One can check that Isabelle successfully verifies all 6 files using the Isabelle command line interface (located at */path/to/Isabelle2021-1/bin/isabelle*) with the command *“build -d. -l*

UnboundedSL" (this command tells Isabelle to build the *UnboundedSL* session, which is defined in the *ROOT* file).

On **Ubuntu**, this can be achieved with the following command (assuming that the file *ROOT* is present in */path/to/artifact*):

```
cd /path/to/artifact
/path/to/Isabelle2021-1/bin/isabelle build -d. -l UnboundedSL
```

On **Windows**, this can be achieved by first running *Cygwin-Terminal.bat* (located at */path/to/Isabelle2021-1/Cygwin-Terminal.bat*), and then:

```
cd /path/to/artifact
isabelle build -d. -l UnboundedSL
```

Expected output:

The first time this command is run, the final lines of the output should look like the following:

```
…
Session Unsorted/UnboundedSL
  /path/to/artifact/AutomaticVerifiers.thy
  /path/to/artifact/Combinability.thy
  /path/to/artifact/FixedPoint.thy
  /path/to/artifact/Properties.thy
  /path/to/artifact/UnboundedLogic.thy
  /path/to/artifact/WandProperties.thy
Running UnboundedSL ...
Finished UnboundedSL (0:00:18 elapsed time, 0:00:55 cpu time, factor 2.95)
0:00:24 elapsed time, 0:00:55 cpu time, factor 2.29
```

This output indicates that Isabelle successfully verified the 6 files in 18 seconds. Because Isabelle caches the results, executing the command again might result in the following final lines:

```
…
Session Unsorted/UnboundedSL
  /path/to/artifact/AutomaticVerifiers.thy
  /path/to/artifact/Combinability.thy
  /path/to/artifact/FixedPoint.thy
  /path/to/artifact/Properties.thy
  /path/to/artifact/UnboundedLogic.thy
  /path/to/artifact/WandProperties.thy
0:00:03 elapsed time
```

A different output might indicate a problem.

b. Using Isabelle's GUI

Note that Isabelle's GUI, which is located at */path/to/Isabelle2021-1/Isabelle2021-1,* 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…).
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.
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 make a proof invalid, but provide help to improve the proof).
- Clear or orange indicates successful verification for this part; Orange indicates a warning (warnings do not make a proof invalid, but help to make the proof better).

Red indicates an error (this should not happen).

(3) Verify the absence of unproven results.

In Isabelle, the only way to "fake" a proof is by using the keyword "sorry". Therefore, one can make sure that all results have been proven by making sure that there are no "sorry" statements; On Ubuntu, this can be achieved with the following command (where *path/to/artifact* should be replaced by the actual path to the artifact):

```
cd path/to/artifact
grep "sorry" *.thy
```

Structure of the Isabelle/HOL formalisation

The artifact contains the following 6 Isabelle files:

- *UnboundedLogic.thy:* Defines the unbounded logic as in section 2, and proves the results of section 2.5 (rules for Hoare triples and frame rule).
- *Properties.thy*: Proves the distributivity and factorisation rules from Fig. 4 (section 2).
- *Combinability.thy*: Defines combinability and proves the rules shown in Fig. 5 (section 3).
- *FixedPoint.thy*: Defines and proves the results from Sect. 4. The induction principle (theorem 5) is called "FP_preserves_subset_property" and can be found at the end of the file.
- *AutomaticVerifiers.thy*: Proves the results from Sect. 5.
- *WandProperties.thy*: Prove useful properties about the magic wand.

Correspondence with the paper

We suggest to use Isabelle's GUI to navigate the formalisation (see point (2) b. in the *Getting Started* part), in order to check that it is consistent with the claims in the paper. To jump to the definition of a term, click on it while holding the Control key.

The table below connects the claims in the paper with the Isabelle/HOL formalisation.

Paper		**Isabelle/HOL formalisation**	
Section	**Element(s)**	**File**	**Element(s)**
2.2	Definitions 1, 2, 3	UnboundedLogic.thy	locale logic (*)
2.3	Assertion language	UnboundedLogic.thy	datatype assertion (**)
	Figure 3		function sat
2.4	Theorem 1 (figure 4)	Properties.thy	many lemmas (***)
2.5	Definition of Hoare triples	UnboundedLogic.thy	lemma valid_hoare_triple
	Theorem 2		theorem frame_rule
3	Definition 4	Combinability.thy	definition combinable
	Theorem 3 (Figure 5)		many lemmas (***)
4.2	Definition 8	FixedPoint.thy	definition subset_property
	Theorem 5		theorem FP_preserves_subset_property
5.1	Figure 6	AutomaticVerifiers.thy	fun syn_mult
	Theorem 6		theorem syn_sen_mult_same
	Rule PackageWand Rule ApplyWand		theorem package_wand theorem apply_wand
5.2	Theorem 7	AutomaticVerifiers.thy	theorem exists_lfp_gfp
	Rule Fold		theorem fold_lfp
	Rule Unfold		theorem unfold_lfp
5.3	Figure 7	AutomaticVerifiers.thy	fun wf_assertion
	Combinability		theorem wf_combine

(*) A “locale” is a way in Isabelle/HOL to define a parametric theory, by fixing some parameters and assuming some axioms. In our case, the locale *logic* corresponds to definitions 1, 2, and 3, with the following correspondence between the paper and the parameters of the locale:

	In the paper	**In the Isabelle/HOL formalisation**
Definition 1	Σ	Type ‘a
	⊕	plus
Definition 2	S	Type ‘b
	+	sadd
	·	smult
	1	one
	Multiplicative inverse	sinv
Definition 3	⊙	mult
	Predicate valid	valid

(**) In the Isabelle formalisation of our assertion language:

- "Sem" is the constructor for semantic assertions
- "Mult" is the constructor for fractional assertions
- "Bounded" is the constructor for the bounding operator
- "Pred" represents the predicate symbol P

(***) For each equivalence, the two directions are proven with two distinct lemmas. The names of the lemmas in the file Properties.thy and the names of the rules in Figure 4 should roughly correspond.