CS 494 – Provably Correct Programming

William Mansky

Questions?

Top

Practical Hoare Logic: Iris

- Tool #2: Iris, a verification framework inside Coq
  - Based on *separation logic*, a version of Hoare logic with support for memory and shared resources
  - Default language is a simple functional language with memory
  - Proofs combine *symbolic execution* of programs with tactics for using/proving facts about resources

- Iris has lots of extensions, applications, and target languges. We'll look at a few!

Separation Logic

- Hoare logic for programs with *memory* (pointers, references, etc.)
- Two new kinds of assertions:

$p \mapsto v$	means “p is a pointer that points to v”
$P * Q$	means “P and Q are true *on separate parts of memory*”

$\{ p \mapsto 2 \wedge q \mapsto 3 \}$ `*p = 4` $\{ p \mapsto 4 \wedge q \mapsto 3 \}$

Not true if $p = q$!

$\{ p \mapsto 2 * q \mapsto 3 \}$ `*p = 4` $\{ p \mapsto 4 * q \mapsto 3 \}$

Separation Logic: Loads and Stores

- Hoare logic for programs with *memory* (pointers, references, etc.)
- Two new kinds of assertions:

$p \mapsto v$ means “p is a pointer that points to v”

$P * Q$ means P and Q are true *on separate parts of memory*

$\{ p \mapsto v \}$ x = *p $\{ p \mapsto v \land x = v \}$

$\{ p \mapsto v \}$ *p = a $\{ p \mapsto a \}$

Separation Logic: Resources

```
H : P
_________
P /\ P

split.

H : P                H : P
_________            _________
P                    P
```

Separation Logic: Resources

$$\frac{H : x \mapsto v}{x \mapsto v * x \mapsto v}$$

Shouldn’t be provable!

If we could split:

$$\frac{H : x \mapsto v}{x \mapsto v} \qquad \qquad \frac{}{x \mapsto v}$$

Separation Logic: Resources

$$\frac{\texttt{H : x} \mapsto \texttt{v}}{\texttt{exists p1 p2 v2 v2, p1} \mapsto \texttt{v1 * p2} \mapsto \texttt{v2}}$$

Shouldn’t be provable!

“two different pointers exist in memory”

We have to “use up” a points-to assertion in order to prove something with it: it’s more like a *resource* than a logical fact

Separation Logic: Resources

- Logical facts like $x = 2$, $x < 5$, etc. stay true when they're true: we don't have to "use them up" to prove things about x
- But points-to assertions *do* get used up!
  - $p \mapsto v$ does *not* imply $p \mapsto v * p \mapsto v$
  - only one function/thread/program at a time can own a piece of memory

- $p \mapsto v$ is more like a *resource* than a logical statement: we can pass it around between functions, but once we use it to prove something, it's gone
- We'll need special tactics to manage resources in a program!

Questions?

Top

Setting Up Iris (version 3.4.0)

- If you installed the Coq Platform, you have it already
- If you installed Coq via OPAM, you can use OPAM to install Iris too (see instructions at https://gitlab.mpi-sws.org/iris/iris/-/tree/iris-3.4.0)
- Otherwise, you'll need to build it from source: clone the repo at https://gitlab.mpi-sws.org/iris/iris/-/tree/iris-3.4.0, and run `make && make install` in that folder

- If it's working, you should be able to run this line in your IDE:
  `Require Import iris.heap_lang.proofmode.`

Setting Up Iris – Special Characters

- There's a lot of fancy notation and special characters in Iris!
- You can find instructions for setting up your editor at https://gitlab.mpi-sws.org/iris/iris/-/blob/master/docs/editor.md
- You can also do `Require Import iris.bi.ascii.` to enable ASCII notations (full list at https://gitlab.mpi-sws.org/iris/iris/-/blob/master/iris/bi/ascii.v)

Iris Resources

- We will be working from a modified version of the Iris Tutorial (https://gitlab.mpi-sws.org/iris/tutorial-popl21)

- A really good overview of the whole system from the ground up is available at https://arxiv.org/pdf/2105.12077.pdf

- There are links to more tutorials and lecture notes at https://iris-project.org/#learning

- A list of tactics is at https://gitlab.mpi-sws.org/iris/iris/-/blob/master/docs/proof_mode.md

Questions?

Top

Feedback

- For today’s exercise, please fill out the anonymous poll at https://forms.gle/Cz3iKEdZ28JR92na7, then submit “finished” or something similar for exercise 3/10

- Don’t hesitate to let me know if there’s anything I can do to help you get more out of the class!

- Thank you! Your feedback helps me make the class better.