

Reasoning About Languages with Binding

Examples, Problems, Solutions

JAIST Workshop
24–25 April, 2005

Version of 22nd April 2005

Long-term goal: Mathematical reasoning presented formally

Why? Machine assistance in:

- checking correctness
 - hardware correctness already a practical application
- developing original work
 - computations (computer algebra), experimenting with alternatives, keeping track of cases, organizing complex arguments, searching for existing lemmas, ...
- communicating work
 - Reader can choose level of detail, preferred notations, ...
- libraries: archiving and searching.
- manipulating arguments
 - Dependencies, generalizing and specializing proofs, ...
- education: all the above especially useful to students

This will happen eventually.

Many developments are needed for this goal to be realized

- Sociological
 - Some change to what is accepted for human readers.
- Foundational
 - Logics more amenable to automation.
 - ...
 - Logics supporting more natural representation of mathematics.
 - ...
 - **Representing and reasoning about binding:**
Nominal logics, FM, Twelf, ...
- Technical
 - Proof search algorithms and heuristics
 - ...
 - **Representing and reasoning about binding:**
 - good representations: Gordon/Melham/Norrish, McKinna/Pollack, Urban's nominal logic in HOL, ...
 - tactics to support representations of binding

Our topic is a part of the overall project of mechanised reasoning.

Many technical approaches proposed to reason formally about languages with binding

- Concrete approaches
 - Curry/Feys, de Bruijn, Stoughton, McKinna/Pollack, Gordon/Melham/Norrish, Hendriks/van Oostrum, ...
- Higher Order Abstract Syntax (HOAS): $(exp \rightarrow exp) \rightarrow exp$
 - LF (Harper, Honsell, Plotkin)
 - Hybrid (Ambler, Crole, Momigliano)
 - Twelf (Pfenning, Shürmann)
 - Miller/McDowell/Tiu
- Weak HOAS: $(atom \rightarrow exp) \rightarrow exp$
 - Context Calculus (Honsell, Miculan)
 - Desperoux/Felty/Hirschowitz
- “Freshness” approaches
 - FM, nominal (Pitts, Gabbay, Urban, Cheney)
 - Schöpp/Stark

Another categorization of these approaches

- Represent binding in well-known logics
 - All the concrete approaches
 - Hybrid
 - All the Weak HOAS approaches
 - Urban's prototype nominal logic in Isabelle/HOL
- New logics, specifically intended for reasoning about binding
 - LF, Twelf, Miller/McDowell/Tiu
 - So far, all freshness approaches except Urban's prototype.

Is it feasible to reason formally about languages with binding?

Can any of these approaches express all the definitions and arguments we want to use?

- Concrete approaches surely can ...
 - ... but at expense of long-winded reasoning.
- Specialised approaches (HOAS, FM) handle binding issues elegantly ...
 - ... but do they extend to the larger goal of mechanised reasoning?
- We also want definitions, statements and proofs to be *natural*. . .
 - ... but we might have to modify our notion of *natural*.
- There is no last theorem.
 - An approach should extend to new problems, and new techniques of proof.

How can we know if an approach is adequate before investing significant effort in using it?

Needed: A challenge problem set for reasoning about binding

- To test technical approaches to reasoning about binding, we suggest developing a challenge problem set.
 - E.g. the **POPLmark Challenge**,
<http://www.cis.upenn.edu/proj/plclub/mmm/>
- When we come across a problem that doesn't work well in existing techniques, we add it to the problem set.
- The challenge problem set should be unified and simple.
 - It should take a few days to develop a solution.

Please suggest problems that give difficulty in some of the established techniques.

Some Naturally Occurring Formalisation Problems

- Eigenvariables: freshness of globally bound variables
- Simultaneous substitution
- Infinite structures; e.g. Böhm trees
- Logical relations

For more details on these examples, see
<http://homepages.inf.ed.ac.uk/rap/>

The last three are not tested by the POPLmark challenge

Technical problems limit applicability of some approaches

- Here are some examples of technical details.
 - Nominal approaches and Weak HOAS interact with Axiom of Choice.
 - The Gordon/Melham/Norrish approach doesn't work in intentional type theory.
 - Using an intentional logic, well-founded recursion does not unfold as desired, so one may need simultaneous substitution to make some definitions structural.
 - The eigenvariable problem disappears using de Bruijn, but statements about variable occurrences in the context (e.g. weakening) become unnatural.
- To know which approaches work in realistic problems, we must do realistic examples.
- Proponents of an approach must be forthcoming in explaining the **strengths** and **weaknesses** of their approach.

Good implementation is essential

- Realistic examples require good implementation support.
- This is more of an issue for specialised logics than for representations in standard logics.
 - Twelf, McDowell/Miller/Tiu, FM, have only prototype implementations.
 - de Bruijn, Honsell/Miculan, Gordon/Melham/Norrish, can be used in logics with well developed implementations.
- Tactics to support a technical approach are also essential.
 - E.g. Norrish's tactics for Gordon/Melham style.
 - **Little else has been done on this as yet.**

Conclusion

- Reasoning about binding is part of a larger programme of formal reasoning.
- To be successful, approaches must handle a wide range of examples and problems.
- Besides a good general approach, support by smart tactics is probably necessary.
- **No current approach makes this a solved problem.**
- The only realistic way to test approaches is to experiment with realistic problems.
- To make this feasible, we should collect naturally occurring examples that cause difficulty in established approaches.
- Hopefully we can develop a unified (but open ended) challenge problem set.