Formally verified programming with monads in Coq

(Formalnie zweryfikowane programowanie z monadami w Coqu)

Zeimer

Praca inżynierska

Promotor: dr Wpisuyashi TODO

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

czerwiec 2019

Abstract

We introduce hsCoq, a Coq library for formally verified general-purpose programming with Haskell-style abstractions: functors, applicative functors, monads, monad transformers and typeclass-based effects. We discuss the design choices we made and illustrate the working of the library with examples taken from [1].

...

Contents

Chapter 1

Introduction

In chapter 1 we motivate the need for formal verification of software and briefly describe the Coq proof assistant. In chapter 2 we discuss the problem of modeling computational effects in programming languages and compare existing approaches. In chapter 3 we present our library hsCoqand discuss its design. In chapter 4 we give some example programs and prove their properties. In chapter 5 we describe our approach to proof engineering - the formalized mathematic's equivalent of software engineering.

Chapter 2

A short introduction to Coq

This chapter briefly introduces the Coq proof assistant to those who are not familiar with it. First we present some motivation for formal verification of hardware, software and mathematics and then describe the underlying theory of Coq.

2.1 Formal verification of hardware and software

Since their invention in the 1940s, computers' significane rose at a very fast pace. They were getting applied to an ever expanding range of problems by more and more people, private companies and governments alike. It shouldn't be a considered a surprise then that we became very reliant on them for both small conveniences and large scale projects.

But significane is not the only thing that rose - another one is complexity. Exponentially growing processing speed required the complexity of chip designs to grow at a similar rate. More complex products and services require more complex software architectures and with new business models, like cloud computing, comes even more complexity in the form of virtualization, containerization and so on.

And with complexity comes, of course, the potential for bugs, which may cause a lot damage. A malfunction in software running the stock exchange can mean billions of dollars of losses; in software running a nuclear power plant - deadly radiation for thousands of people and energy shortage for millions more.

Due to these dangers a lot of effort has been put into assuring that hardware and software are correct and with great success, but here and there bugs still have crept in. Some of the most spectecular were, recently:

- Metldown, which "exploits side effects of out-of-order execution on modern processors to read arbitrary kernel-memory locations including personal data and passwords." [2]

- Spectre, which uses speculative execution and branch prediction to "leak the victim's confidential information via a side channel to the adversary." [3]
- Heartbleed, which "allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet" [4]

DeepSpec [5] is a Coq-based project that tries to eliminate both hardware and software bugs and security vulnerabilities by creating a web of formally verified hardware, operating systems, compilers, web servers, cryptography libraries etc.

2.2 Formal verification of mathematics

Hardware and software are not the only things in need of formal verification - mathematics is also one of them.

The four colour theorem is a problem posed in 1852. It states that any planar map can be coloured with only four colours so that no two regions sharing a boundary are assigned the same colour. It became famous for resisting many proof attempts by many famous mathematicians for more than a century until it was finally proved by Appel and Haken in 1976. Its importance stems from the proof method - it was the first major theorem proven using a computer program, whose job was to make sure a very large case analysis was exhaustive.

Thomas Tymoczko, a philosopher of mathematics, criticised this proof by labeling it with a term he invented just for this purpose - "non-surveyable". He considered a proof to be non-surveyable when its verification cannot be performed by human mathematicians competent in the relevant field. Appel and Haken's proof certainly did fail the surveyability criterion - the program was written in IBM 370 assembly, a language graph theorists very likely didn't understand.

This was the perfect theorem to let formal proofs and formally verified programs shine by dispeling Tymoczko's and other mathematician's doubts. This is what indeed happened in 2005, when Georges Gonthier presented a proof of the theorem formalized in Coq [6] [7].

But big theorems with difficult proofs are not the only call for formalized mathematics. Another one is the mere fallibility of humans, especially their limited memory and reasoning skills and the tendency to follow authority. As unmathematical as it sounds, these are the main reasons cited by Vladimir Voevodsky, a field medalist mathematician turned a fan of formal proofs, in one of his talks [8].

The fields he refers to are homotopy theory, higher category theory and motivic cohomology - all of them containing many layers of abstraction, tons of concepts and definitions, and rather shaky foundations.

As an example, noticing an error in one of his papers took 7 years and repairing

the mistake another 6 years. In another, more extreme case, after publishing a paper in 1989, an alleged counterexample was found in 1998 by anoter expert in the field, but it was too difficult for them to agree on whether it really was a counterexample and Voevodsky only realized he was wrong in 2013. All of this put him in search of formalized foundations of mathematics, and he chose Coq to purse them.

2.3 The Coq proof assistant

Coq [9] is a piece of software implementing a formal system whose slight variants go under a plethora of names: Calculus of (Inductive) Constructions, (Intensional) Martin-Löf Type Theory, Intuitionistic Type Theory, Constructive Type Theory, etc.

Thanks to the Curry-Howard correspondence [**?**] Coq can be seen as both a functional programming language and a proof assistant.

Chapter 3

Computational effects

Chapter 4

Design

Chapter 5

Examples

Chapter 6

A case study in proof engineering

Chapter 7

Conclusion

Chapter 8

TODO

1. Introduction: functional programming, formally verified programming and proving.
2. Approaches to computational effects: chaos, ML-style, monads, algebraic effects.
3. A description of the inner workings of the library: design choices, file structure, implementation.
4. Examples: some from Just Do It, maybe some custom ones.
5. Safety: some theorems and proofs.
6. Theoretical comparison of the ease of use with Haskell and Idris.
7. Practical comparison with MERC.
8. Cite some literature: some Coq papers, Moggi, Just Do It, Experimenting with Monadic Equational Reasoning in Coq
9. Technical matters:
   (a) Mention where's the implementation and put it to Coq's repository of user libraries.
   (b) Installation guide.
   (c) Tools: why no ssreflect?
   (d) Documentation (it's in the source code).
10. More: a case study in proof engineering - how do the tactics hs, monad and (maybe) the one for reflective functor simplifcation work?
11. Deficiencies, conclusion and further work.
12. Points to make: this is a library for general purpose programming, without some deep goal.

Bibliography

[1] Jeremy Gibbons and Ralf Hinze,
Just do It: Simple Monadic Equational Reasoning, 2011
`http://www.cs.ox.ac.uk/jeremy.gibbons/publications/mr.pdf`

[2] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom and Mike Hamburg,
Meltdown: Reading Kernel Memory from User Space, 2018
`https://meltdownattack.com/meltdown.pdf`

[3] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz and Yuval Yarom,
Spectre Attacks: Exploiting Speculative Execution, 2019
`https://spectreattack.com/spectre.pdf`

[4] `www.heartbleed.com`, 2019

[5] `www.deepspec.org`, 2019

[6] Georges Gonthier, *A computer-checked proof of the Four Colour Theorem*, 2005
`https://www.cl.cam.ac.uk/~lp15/Pages/4colproof.pdf`

[7] Georges Gonthier, *Formal Proof - The Four-Color Theorem*, 2008,
`http://www.ams.org/notices/200811/tx081101382p.pdf`

[8] Vladimir Voevodsky, *UNIVALENT FOUNDATIONS*, slides for a talk given at IAS on 26 March 2014,
`http://www.math.ias.edu/~vladimir/Site3/Univalent_Foundations_files/2014_IAS.pdf`

[9] Coq Development Team, *The Coq Proof Assistant Reference Manual*, 2019