Effectful programs and their proofs in a dependently-typed setting

Pierre-Evariste Dagand

This internship stands at the crossroad between MPRI 2.4 (“Functional programming and type systems”), MPRI 2.7.2 (“Proof assistants”) and MPRI 2.36.1 (“Proofs of programs”). If you take a non-trivial subset of these courses, then this is your opportunity to become a one-man band, playing with monads, type theory and separation logic!

Have a look at CompCert’s SimplExpr\(^1\). In the last part of MPRI 2.4, I will tell you that this is a monadic program, allowing Xavier Leroy to (safely) access an effectful gensym operation in an otherwise pure programming language.

Now, look at its associated correctness proof\(^2\) and, in particular, the supporting specification\(^3\) lemmas. In MPRI 2.36.1, you would probably have been told that the separation properties alluded to in the specification file are indeed the ingredients necessary to setup a separation logic.

However, it does not take a semester of MPRI 2.7.2 to notice that these structures (monads for programming, separation logic for reasoning) intertwine in the proof: the proof carries over the purely functional representation of the monadic program, thus managing the monadic, logical and sub-structural invariants all at once. Automating such a proof is a daunting task, and rightfully so!

By combining concepts and techniques from these three domains, I offer to:

1. Streamline the implementation and proof of the SimplExpr module. A measure of success will be given by the length of the resulting proof as well as its resilience to changes;

2. Generalize the approach to the other monads used in CompCert. A measure of success will be given by the ease with which new use cases are supported;

3. Develop a formal understanding of separation logics for monadic programs. A concrete result of this work would be a generic library for specifying monads and their logics as well as offering support for automated reasoning.

---

\(^1\)http://compcert.inria.fr/doc/html/compcert.cfrontend.SimplExpr.html
\(^3\)http://compcert.inria.fr/doc/html/compcert.cfrontend.SimplExprspec.html