Foundational Proof Certificates

Making proof universal and permanent

Dale Miller
INRIA-Saclay & LIX/École Polytechnique
dale.miller at inria.fr

Abstract

Consider a world where exporting proof evidence into a declarative, universal, and permanent format is taken as "feature zero" for computational logic systems. In such a world, provers will be able to communicate and share theorems and proofs; libraries can archive and organize proofs; and marketplaces of proofs would be open to any prover that admits checkable proof objects. In that world, proof checkers must be entrusted with the task of checking whether or not such proof evidence elaborates into a formal proof. A key to developing such a universal and permanent approach to proof evidence is the selection of an appropriate logical framework for defining the semantics of proof evidence [5].

Recent developments in structural proof theory provide a foundational approach to *proof certificates*. In particular, the *focused proof systems* LJF, LKF, and LKU for classical and intuitionistic logics [3, 4] can be fashioned into a high-level and declarative framework for defining the semantics of a wide range of proof evidence [6]. The resulting framework is an approach to *foundational proof certificates* (FPCs) that provides precise descriptions of proofs that are both independent of the technology that produced them as well as flexible enough to allow encoding a rich collection of proof structures such as, for example, Frege proofs, natural deductions, resolution refutations, and Herbrand disjunctions.

The λProlog programming language [7] is an appropriate programming language for implementing a checker for FPC (over first-order logic proofs) and for specifying the semantics of proof evidence. While λProlog contains typing, abstract datatypes, and higher-order programming in a style similar to ML—the first programming language designed for implementing proof checkers [2]—it goes beyond ML by providing a logically clean notion of binding and (object-level) substitution. Furthermore, λProlog implements both unification and backtracking search, two features critical for implementing proof reconstruction. These two features will allow proof certificates to have the option of eliding some proof evidence in the hope that the proof checker can reconstruct the missing details. Allowing a trade-off between certificate size and checking (and proof reconstruction) time is a valuable aid in designing flexible proof certificate formats [1].

The progress and plans for the ProofCert [5] project within the Parsifal team at INRIA will be presented in this talk.

Acknowledgments. This work is funded by the ERC Advanced Grant ProofCert.

Categories and Subject Descriptors F.4.1 [*Mathematical Logic*]: Proof theory

General Terms Formal proofs, proof checking

Keywords proof certificates, focused proof systems

References

[1] Z. Chihani, D. Miller, and F. Renaud. Foundational proof certificates in first-order logic. In M. P. Bonacina, editor, *CADE 24: Conference on Automated Deduction 2013*, LNAI 7898, pages 162–177, 2013.

[2] M. J. Gordon, A. J. Milner, and C. P. Wadsworth. *Edinburgh LCF: A Mechanised Logic of Computation*, LNCS 78. Springer, 1979.

[3] C. Liang and D. Miller. Focusing and polarization in linear, intuitionistic, and classical logics. *Theoretical Computer Science*, 410(46):4747–4768, 2009.

[4] C. Liang and D. Miller. A focused approach to combining logics. *Annals of Pure and Applied Logic*, 162(9):679–697, 2011.

[5] D. Miller. Proofcert: Broad spectrum proof certificates. An ERC Advanced Investigator Grant funded for the five years 2012-2016. Feb. 2011.

[6] D. Miller. A proposal for broad spectrum proof certificates. In J.-P. Jouannaud and Z. Shao, editors, *CPP: First International Conference on Certified Programs and Proofs*, LNCS 7086, pages 54–69, 2011.

[7] D. Miller and G. Nadathur. *Programming with Higher-Order Logic*. Cambridge University Press, June 2012.

LFMTP '13, September 23, 2013, Boston, MA, USA.
Copyright is held by the owner/author(s).
ACM 978-1-4503-2382-6/13/09.
http://dx.doi.org/10.1145/2503887.2503894