Structured Presentation of Formal Proofs: an Experiment with Isabelle

F. Kammüller, G. Keller, M. Simons, M. Weber
Forschungsgruppe Softwaretechnik
TU Berlin

The intelligible presentation of formal proofs is usually not attempted because of their technical detail. This formal noise hides the line of reasoning that can be followed and understood by humans. We are investigating methodologies and machine support for presenting formal proofs in an intelligible and structured manner while keeping them amenable to a check by a machine or an interactive development. To this end, we have in the past carried out sizable experiments with an implementation of the logical framework Deva, a descendant of the AUTOMATH family of languages [WSL93, SBR94, AJS94, Web94]. The experiments were carried out in the context of formal software development as well as mathematical proofs.

Although Deva served its purpose as an experimental prototype very well, it turned out to be, in the long run, too monolithic and inflexible (for instance, the module mechanism was internalized into the meta-logic). Still, we think that the various concepts that underlie the specific approach we chose for the presentation of formal proofs in Deva are of a general nature. We are currently trying to apply this approach to proofs expressed in other logical frameworks, Isabelle in particular, and we continue to investigate theoretical aspects of expressing formal proofs. More specifically:

- We are experimenting with notations and calculi for expressing proofs that try to capture algebraic properties underlying proof construction and that allow to express proof refinements. The guiding idea here is to view theorem proving as the process of refining a theorem to its proof. Each refinement step adds more technical detail to the overall proof. With respect to proof presentation, only the first levels of refinements are of interest to a reader. The other refinements can safely be hidden and carried out interactively or completely automatic. Early investigations of tentative calculi uncovered a close relationship with algebraic semantics of substructural logics [DSH93], e.g., full Lambek algebras (FL-Algebras).

- We investigate prototypical implementations of such calculi with "programmable" logical-frameworks such as Isabelle or λProlog as a basis. A first experiment is described in [Kam95] where FL-Algebras are formalized on top of

Isabelle's Pure theory and proof constructions are expressed as FL-Algebra terms. Tactics are designed to automatically prove „validity-properties". The advantage of this approach to constructing prototypical implementations is that one can make use of the structural facilities provided by the logical framework without having to develop them from scratch.

- We are developing prototypical tools that aid in the generation of structured and literate Isabelle proofs in order to demonstrate the viability of our approach to the presentation of formal proofs. One tool [Kel94] allows calculational proofs to be easily performed with Isabelle through an Emacs interface. Some requirements for tool-support that allows hierarchically structured proofs to be interactively developed and documented with Isabelle are investigated in [Kel95].

In the full paper, we will give a more detailed overview of these activities and then focus on our experiences with Isabelle gained during the experiment formalizing FL-Algebras.

References

[AJS94] M. Anlauff, S. Jähnichen, and M. Simons. A support system for formal mathematical reasoning. In Naftalin et al. [NDB94], pages 421–440.

[DSH93] K. Došen and P. Schroeder-Heister, editors. *Substructural Logics*. Oxford Science Publications, 1993.

[Kam95] F. Kammüller. Konstruktion eines Unterstützungssystems für Gral in Isabelle. Diplomarbeit, TU Berlin, Fachbereich Informatik, 1995.

[Kel94] G. Keller. An experimental system for the production and presentation of formal proofs. Studienarbeit, TU Berlin, Fachbereich Informatik, 1994.

[Kel95] G. Keller. Unterstützung hierarchisch Beweise mit Hilfe eines interaktiven Theorembeweisers. Diplomarbeit, TU Berlin, Fachbereich Informatik, 1995.

[NDB94] M. Naftalin, T. Denvir, and M. Bertran, editors. *FME'94: Industrial Benefits of Formal Methods*. Springer-Verlag, 1994.

[SBR94] M. Simons, M. Biersack, and R. Raschke. Literate and structured presentation of formal proofs. In E.-R. Olderog, editor, *IFIP Working Conference on Programming Concepts, Methods and Calculi (PROCOMET'94)*, pages 61–81. North Holland, 1994.

[Web94] M. Weber. Literate mathematical development of a revision management system. In Naftalin et al. [NDB94], pages 441–460.

[WSL93] M. Weber, M. Simons, and Ch. Lafontaine. *The Generic Development Language Deva: Presentation and Case Studies*, volume 738 of *Lecture Notes in Computer Science*. Springer-Verlag, 1993.

Some papers are available in the WWW under the URL `http://www.cs.tu-berlin.de/~car/`.