Porting the HOL Light Analysis Library: Some Lessons (Invited Talk)

Lawrence C. Paulson
University of Cambridge, UK
lp15@cam.ac.uk

Abstract

The HOL Light proof assistant is famous for its huge multivariate analysis library: nearly 300,000 lines of code and 13,000 theorems. A substantial fraction of this library has been manually ported to Isabelle/HOL. The Isabelle analysis library contains approximately 7400 named theorems, including Cauchy's integral and residue theorems, the Liouville theorem, the open mapping and domain invariance theorems, the maximum modulus principle and the Krein–Milman Minkowski theorem.

Why port proofs manually given so much work on porting proofs automatically? Typical approaches rely on low level encodings that seldom yield natural-looking results. Manual porting has allowed us to generalise many results from n-dimensional vector spaces to metric or topological spaces. The transition from the traditional LCF/HOL proof style (which has hardly changed since 1985) to structured proofs has produced a dramatic improvement in the legibility of the material. Automatic porting generally yields a list of theorem statements but no intelligible proofs.

This project has highlighted three features of Isabelle working well together: heuristic automation, structured proofs and sledgehammer. Heuristic automation builds in a lot of implicit knowledge, which is potentially unpredictable, but in combination with structured proofs any breakages (caused by updates to the system) are localised and easily fixed. Sledgehammer (which uses powerful external automation to solve subgoals) can frequently complete an argument without requiring a precise reproduction of the original HOL Light proof. Sledgehammer also encourages a style in which the user reaches the desired result by suggesting a series of intermediate claims.

Such proofs are genuinely human-oriented. And only such proofs will attract mathematicians; even a guarantee of correctness will not impress them unless the system lets them understand and tinker with their formal proofs.

Categories and Subject Descriptors

F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic - Mechanical theorem proving; I.2.3 [**Artificial Intelligence**]: Deduction and Theorem Proving - Deduction (e.g., natural, rule-based)

Keywords HOL Light; Isabelle; proof porting; formalised mathematics

Biography

Lawrence C. Paulson is Professor of Computational Logic at the University of Cambridge, where he has held established positions since 1983. He has written nearly 100 refereed conference and journal papers as well as four books. He introduced the popular Isabelle theorem proving environment in 1986, and made contributions to the verification of cryptographic protocols, the formalisation of mathematics, automated theorem proving technology, and other fields. He has supervised over 20 postgraduate students and numerous postdoctoral researchers. In 2008, he introduced MetiTarski, an automatic theorem prover for real-valued functions such as logarithms and exponentials. He has the honorary title of Distinguished Affiliated Professor from the Technical University of Munich and is an ACM Fellow.

CPP'17, January 16–17, 2017, Paris, France
ACM. 978-1-4503-4705-1/17/01...$15.00
http://dx.doi.org/10.1145/3018610.3023366