Automation for Interactive Proof

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Interactive proof tools such as HOL, Isabelle and PVS support rich formalisms based upon higher-order logic. Researchers have used them to verify hardware and software, but these tools demand much effort from their users. Automatic theorem-provers such as SPASS are powerful, but their use of first-order logic limits their scope. Combining these technologies effectively is not easy. Merely allowing automatic provers to be invoked from an interactive tool, as others have done, imposes on the user the task of preparing the problems.

Our project combines Isabelle with the automatic provers E, SPASS and Vampire. Our conception differs from previous attempts in several respects:

- *One-click invocation*.
- *Automatic selection of lemmas* from the thousands that are available.
- *Multiprocessing*: multiple subgoals and different provers, proof strategies or lemma sets can be tried simultaneously.
- *Proof reconstruction*: the proof, once found, is presented in source form, ready for insertion into the proof script.

Each of these objectives is aimed at reducing the tedium and frustration typical of interactive proof by shifting the workload onto the computer.

Our project has fully achieved its objectives. A simple relevance filter identifies a few hundred of the many thousand theorems available in the Isabelle session. Special features of higher-order logic, such as type classes and polymorphism, are translated into first-order logic. Subgoals and lemmas are sent to automatic theorem provers running in separate processes. Proofs are analysed to extract the list of lemmas actually used. Proof reconstruction works by supplying this list to Joe Hurd's Metis prover. We have performed a vast number of experiments in order to perfect the design.

The outcome of our project is known to the Isabelle community as the Sledgehammer tool. Sledgehammer has become indispensable to Isabelle users, especially novices. Sledgehammer continues to be developed and refined, for example, in its support for higher order logic.

This £249,905 project was funded by the EPSRC [grant number GR/S57198/01].

EPSRC
Engineering and Physical Sciences Research Council

The Team

Jia Meng, the project student, earned a PhD for her work on the translation of Isabelle subgoals into a form suitable for automatic provers.

Claire Quigley, who has a PhD at the University of Glasgow, wrote the code to invoke automatic theorem provers and report their results.

Kong Woei Susanto, another Glasgow PhD, joined the project at its midpoint. He combined Joe Hurd's Metis prover with Isabelle. Metis serves as the basis for proof reconstruction.