Formalization of Mathematics and Automated Reasoning

Noboru ENDO
Professor, Dr. Eng.
Email : endon@gifu-nct.ac.jp

Research Fields Formalized Mathematics, Automated Reasoning

Keywords Mizar, Proof checker, Formalization

Research Outline

Automated Reasoning

Automated reasoning is concerned with the building of computing systems that automate to make inferences. Although the overall goal is to mechanize different forms of mathematical reasoning, the term has been identified with valid deductive reasoning as practiced in mathematics and formal logic. In this respect, automated reasoning is analogous to mechanical theorem proving. Building an automated reasoning program means providing an algorithmic description to a formal calculus so that it can be implemented on a computer to prove theorems of the calculus in an efficient manner.

Applications of Automated Reasoning

Automated reasoning has reached the level of maturity where theorem proving systems and techniques are being used for industrial-strength applications. One such application area is the formal verification of hardware and software systems. The idea behind formal verification is to rigorously prove with mathematical certainty that the system functions as specified. Common applications to hardware design include formally establish that the system functions correctly on all inputs, or that two different circuits are functionally equivalent. One way to increase the quality of software is to supplement traditional methods of testing and validation with techniques of formal verification. The basic approach to formal verification is to generate a number of conditions that the software must meet and verify them by mathematical proof. As with hardware, automated formal verification is concerned with discharging these proof obligations using an automated theorem prover.

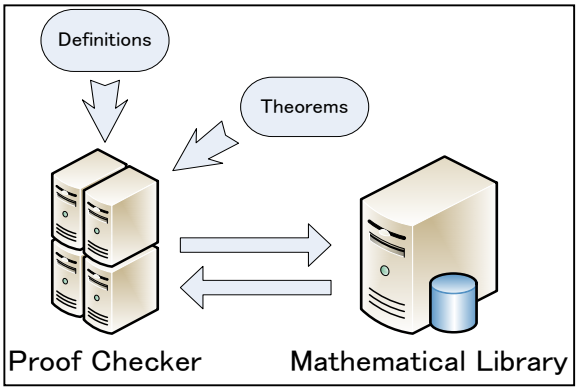
The formal verification of security protocols is an almost ideal application of automated theorem proving in industry. Since the specification of a security protocol is relatively small and well defined but its verification is certainly non-trivial, automated theorem proving is effective working.

One of the main goals of automated reasoning has been the automation of mathematics. An early attempt at this was Automath which was the first computer system.

Mizar Project

The Mizar system is based on Tarski-Grothendieck set theory and, like Automath, consists of a formal language which is used to write mathematical theorems and their proofs. The Mizar Project was started around 1973 by Andrzej Trybulec as an attempt to reconstruct mathematical vernacular so it can be checked by a computer. Its current goal, apart from the continual development of the Mizar System, is the collaborative creation of a large library of formally verified proofs, covering most of the core of modern mathematics. This is in-line with the influential QED manifesto.

Currently the project is developed and maintained by research groups at Białystok University, Poland, the University of Alberta, Canada, and Shinshu University, Japan. While the Mizar proof checker remains proprietary, the Mizar Mathematical Library is licensed open-source.



The distinctive feature of the Mizar language is its readability. As is common in mathematical text, it relies on classical logic and a declarative style. Mizar articles are written in ordinary ASCII, but the language was designed to be close enough to the mathematical vernacular that most mathematicians could read and understand Mizar articles without special training.

For a proof to be admitted, all steps have to be justified either by elementary logical arguments or by citing previously verified proofs. This results in a higher level of rigor and detail than customary in mathematical text-books and publications.