Interactive Theorem Proving

Jeremy Avigad
Departments of Philosophy and Mathematical Sciences
Carnegie Mellon University

Abstract

In computer science, "formal verification" refers to the use of formal methods to verify correctness. This can mean verifying that hardware or software design meets its specification, but it can also mean verifying the correctness of a mathematical proof.

One method of doing the latter is to use an "interactive proof assistant", which is designed to help the user construct a formal axiomatic proof. The user comes to the system with a proof in mind; the system parses the user's input, keeps track of definitions, manages a library of background knowledge, fills in low-level details, carries out and checks long calculations, and, if all goes well, certifies the proof.

The technology is not yet "ready for prime time", but recent experience has shown that it is viable, and a number of interesting verification projects are currently underway. These include Thomas Hales' "Flyspeck" project, which is verifying results in discrete geometry that include his 1998 proof of the Kepler conjecture; Georges Gonthier's project to verify the Feit-Thompson theorem; and Vladimir Voevodsky's development of "univalent" homotopy type theoretic foundations for algebraic topology.

In this series of lectures, I will survey the new technology and describe some of the logical ideas behind it. In particular, I will discuss formal languages, logical frameworks, search procedures, decision procedures, combination procedures, type inference, verified computation, and reflection. I will explain how the field's success relies crucially on the understanding of mathematical reasoning that emerged from fundamental advances in mathematical logic in the twentieth century, and I will argue that its future success requires further theoretical developments in mathematical logic.

To illustrate some of these ideas, I will discuss a formal analysis of the geometric proofs in Euclid's *Elements*, which shows that even diagrammatic reasoning is susceptible to formal methods.