Computer-Hindered Verification (Humans Can Do It Too)

Abstract

Leslie Lamport

Digital Equipment Corporation

Writing proofs is easy. It is so easy that mathematicians and computer scientists seem to have little difficulty writing proofs of incorrect theorems. We need to make it harder to prove things that aren't true. There is an inevitable conflict between the goals of making a proof easy to write and making it likely to be correct. Ordinary mathematical proofs are easy to write, but error prone. Mechanical proof checkers can make it almost impossible to prove an incorrect theorem, but they make it very difficult to prove a correct one. Little attention has been paid to proof methods that lie between these two extremes.

Hierarchically structured hand-checked proofs are more likely to be correct than conventional, unstructured proofs. A modest amount of extra effort in writing the proof yields an enormous increase in confidence compared with ordinary mathematical proofs. By increasing the depth of a hierarchically structured proof, one can increase the likelihood that it is correct. We do not know how reliable such proofs can be. It is possible that they can be made almost as error free as mechanically checked proofs.

Even if hand proofs can be made very rigorous, mechanical verification will still be appropriate for some applications. However, what is proved should depend on the application, not on the limitations of the verification system. The properties to be proved should be expressed in a formalism that is appropriate to the problem. It is then possible to decompose the proof so that different parts are proved by different methods–some mechanically, others by hand. The proof method can depend on the formal structure of the particular property and on how important that property is. For an avionics system, one might use three different methods to prove that (i) the load on a wing is never great enough to make it fail, (ii) a landing is never attempted before the landing gear has been lowered, and (iii) the coffee maker never overheats the coffee.