National Aeronautics and Space Administration

Automated Theorem Prover Axiom Management

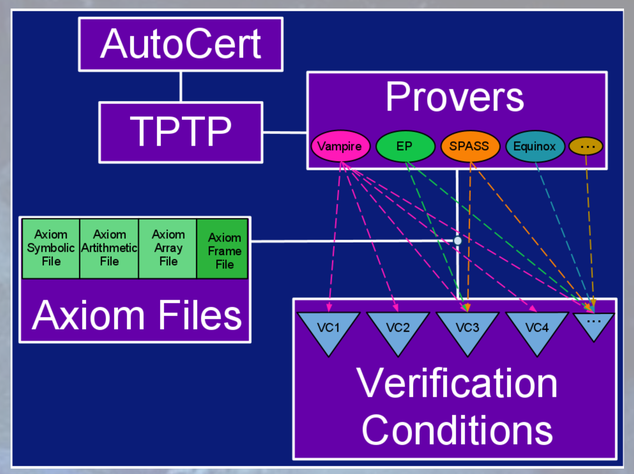
Ashley Holeman[1,2], Ewen Denney[3]

(1) Department of Mathematics, California State University San Bernardino
(2) STAR CESaME, California Polytechnic State University
(3) NASA Ames Research Center, Robust Software Engineering

Introduction

Automated Theorem Provers (ATPs) are computer programs that use collections of axioms which are logical statements assumed to be true, in order to prove conjectures. NASA uses these programs to verify safety and functional requirements in domains like Guidance, Navigation, and Control. This is often a challenge from a verification perspective due to its complex and mathematical nature. Originally the axiom-frame was created to verify a specific software, however they continued to use and expand the file over the duration of numerous projects. Currently in the axiom-array file there are at least 30 axioms on each major topic, including the theory of coordinate systems, elementary arithmetic and linear algebra. Provers have evolved and become more efficient over time rendering many of the axioms unnecessary. One task is to manage the axioms by arranging them into logical sections, deleting ones that are no longer required and rewriting some into a more general case. This will help reduce the time required to run the provers, resulting in a more efficient program. Each change done to the axiom file must be checked in order to verify that the original conjectures can still proven true.

How it Works



- **AutoCert** : a system built by NASA used for verifying safety and functional requirements.
- **TPTP**: Thousands of Problems for Theorem Provers is a library of test problems for ATP systems.
- **Provers**: ATP systems that use first order logic to prove conjectures.
- **Axiom Files**: Consist of numerous logical statements that are assumed to be true.
- **Verification Conditions**: Lemmas that must be verified in order to prove a larger conjecture.

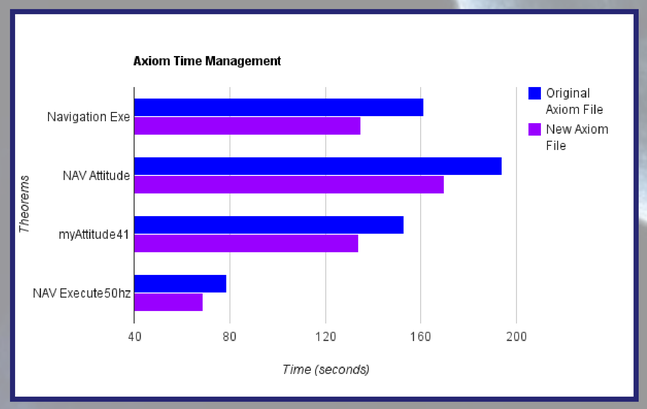
Acknowledgements

Science Teacher And Research (STAR) Program

Center for Excellence in Science and Mathematics Education (CESaME)

This material is based upon work supported by the S.D. Bechtel, Jr. Foundation and by the National Science Foundation under Grant No. 0952013. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the S.D. Bechtel, Jr. Foundation or the National Science Foundation.

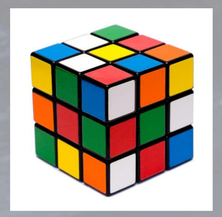
Results



Time is always an important factor when running programs. Cleaning up the axiom-frame file by deleting duplicates, unneeded axioms, and rewriting axioms into a more general case helped decrease the time it takes to run the program. This resulted in a more efficient software verification program for NASA . The initial timed results using the original axiom-frame file took about ten minutes to run. After the numerous changes to the axiom-frame it ran in just under eight and a half minutes, saving anywhere from 10 to 25 seconds on each theorem being testing.

Other Application of ATP

A Rubik's cube that has been rearranged into disorder can be turned into a conjecture and proved using axioms that describe the legal changes that one can make to the cube's alignment.



The proof would outline the sequence of moves needed in order to solve the cube.