

Visitor Research Report

Visitor Name: Mr. Timothy E. Wang
Georgia Institute of Technology

Area of Research: Formal Verification of Adaptive Controllers

Period of Visit: May 11, 2009 – July 31, 2009

Goal:

The long term goal of the project is to provide a framework to build high-confidence control software systems and eventually moving towards certifying adaptive controllers. The short term goal is to formalize control theories in a theorem prover.

Strategy:

The current strategy pursued is theoretically sound. The link between the Lyapunov stability theory and invariants of the hoare framework is well established. Proofs on the specification level can be translated so far by hand to the code level for specific examples. It's envisioned that in the future an autocoder environment like that of Simulink/RTW can be enhanced with such capability. Currently the proofs are hand written on the specification level and as well on the C level. To go from one level to another we first want to formalize a piece of control code (either in matlab or in simulink diagram form) in a theorem prover such as PVS. The selection of PVS is influenced by the NASA Langley formal methods team. A library of control theories should be developed first to support the analysis of the formalized control software system. For linear systems with simple linear controllers only linear algebra and linear vector spaces theories are needed.

Accomplishments:

Developed a vector space/linear algebra library based on the existing NASA PVS algebra library. Used the library for the proof checking and analysis of a simple PID controller code.

Future Work:

Need to automate the process from matlab diagram to PVS (create semantics for all the continuous blocks). Need to demonstrate an autocoder framework that can generate proof along with the code from the block diagrams. Extend current idea of ellipsoid invariants to adaptive controller code.

Pending Publications:

Seminar Presented: *Formal Analysis of Control Software: Guaranteeing Control Properties From Specification to Code* at NIA on 07/31/2009