Project Overview

Goal: increase software reliability
Approach: specifications for formal, informal reasoning
Problem: specifications are typically absent
  • programmers are reluctant to write them
  • programmers are not very good at writing them
  • too few tools accept them as input
Solution: automatically infer program specifications
Application: Erdős internet agent system from NTT
Daikon system (tool for generating specifications)
  • 9 new releases at http://pag.lcs.mit.edu/daikon/
Theorem-proving
  • Automate Isabelle proofs over IOA language
    • Automatically propose lemmas
    • Automatically select tactics
Temporal invariants: 3 techniques
  • Results from all 3 implementations
  • commercial apps, Java libraries, Erdös programs
Support tools and users; make research results broadly available

Additional experiments on NTT's Erdös agent system
  • Collaboration with Tadashi Araragi of NTT
  • Need additional programs

Follow up and extend previous successes
  • Theorem-proving via Isabelle, ESC/Java, others
  • Temporal invariants for agent and other programs