MIT2001-01: Dynamic Invariant Detection for Program Understanding and Reliability

Michael Ernst

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: Erdös internet agent system from NTT

MIT2001-01: Dynamic Invariant Detection for Program Understanding and Reliability

Michael Ernst

Progress Through June 2002

Daikon system (tool for generating specifications)

- 7 new releases at http://pag.lcs.mit.edu/daikon/
- integrate research results; support users

Theorem-proving

- Java language and ESC/Java static checker
- IOA language (distributed algorithms)
    - largely automatic proofs; reduce human burden
    - joint with Theory of Distributed Systems group

Temporal invariants

- Preliminary results, applied to commercial programs

Research Plan for the Next Six Months

Support tools and users; make research results broadly available

Perform experiments directly on NTT's Erdös agent system from NTT, or collaborate with NTT researchers

Integrate with (automatable) Isabelle theorem-prover

Extend detection of temporal invariants