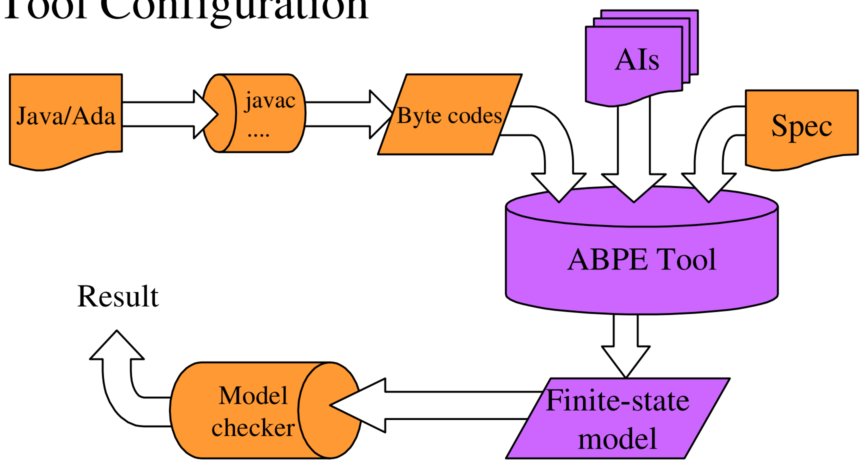
Model Construction for Finite-State Verification

Application of Abstract Interpretation and Partial Evaluation Techniques

Tool Configuration



New Ideas

- Partial evaluation (PE) can transform complex language constructs into a form that is amenable to finite-state modeling.
- Abstract Interpretation (AI) can reduce the size of a system's state space while preserving information necessary for analysis.
- Unlike in traditional applications, for verification a systems "execution semantics" need not be preserved during analysis and transformation.
- Abstract Interpretation-based Partial Evaluation (ABPE) can compile source code into safe, compact finite-state models suitable for verification.

Impact

- Finite-state verification (FSV) techniques, e.g., model checking, are difficult to apply to software systems because of the need to "hand build" system models.
- ABPE automates model construction.
- ABPE guarantees correctness of resulting models.
- ABPE scales to real-world, component-based systems described in mainstream programming languages.
- Thus, ABPE will enable reliable use of FSV technology on real-world systems by non-experts.

Schedule

1998 — 1999 — 2000

1998–1999

- Prototype byte-code PE tool.
- Develop foundations of AI-based PE.
- Apply and assess effectiveness of PE tool for preparing FSV tool inputs.

1999–2000

- Enhance PE prototype with support for abstractions.
- Apply and assess effectiveness of ABPE for preparing FSV tool inputs.

K-STATE Kansas State University™

Schmidt, Dwyer & Hatcliff

NASA