PASS

Björn Wachter
Lijun Zhang
Holger Hermanns

Universität des Saarlandes

Motivation

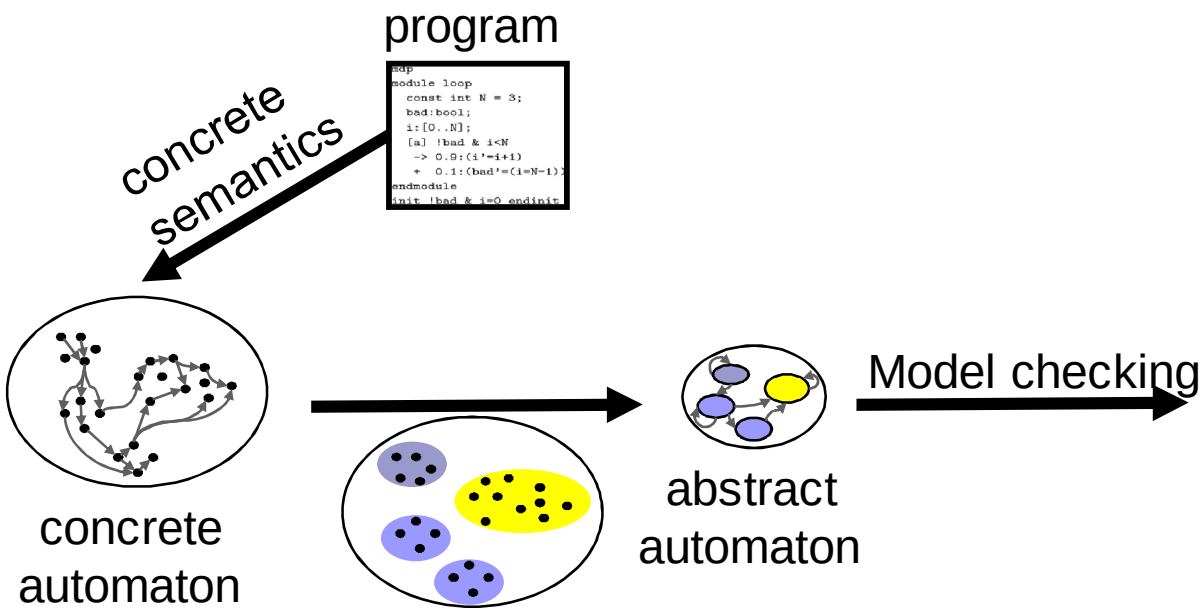
- **Probabilistic MC** (model checking)
  - Embedded systems: interaction with physical environment
  - Networked systems: message loss
- Many of those are infinite-state
  - Software
  - Time
- **However:**
  - Infinite-state model checkers: no probability
  - Probabilistic model checkers: only finite-state, not SW

Combine abstractions for SW MC with stochastics!

- **Predicate abstraction**: software model checkers SLAM, BLAST

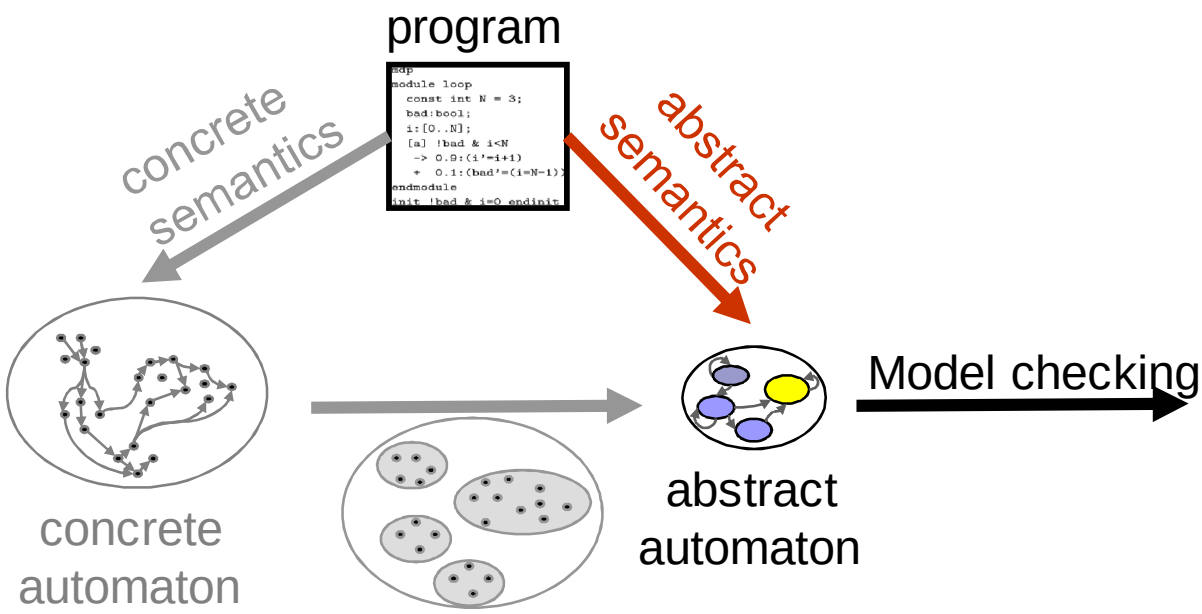
Previous Work: Abstraction & Probabilistic Model Checking

- Previous Work:
  - e.g. dÁrgenio (PAPM-PROBMIV01/02), Kwiatkowska (Qest06), de Alfaro (CAV07)
  - **what if concrete automaton is large/infinite?** $\models \varphi$



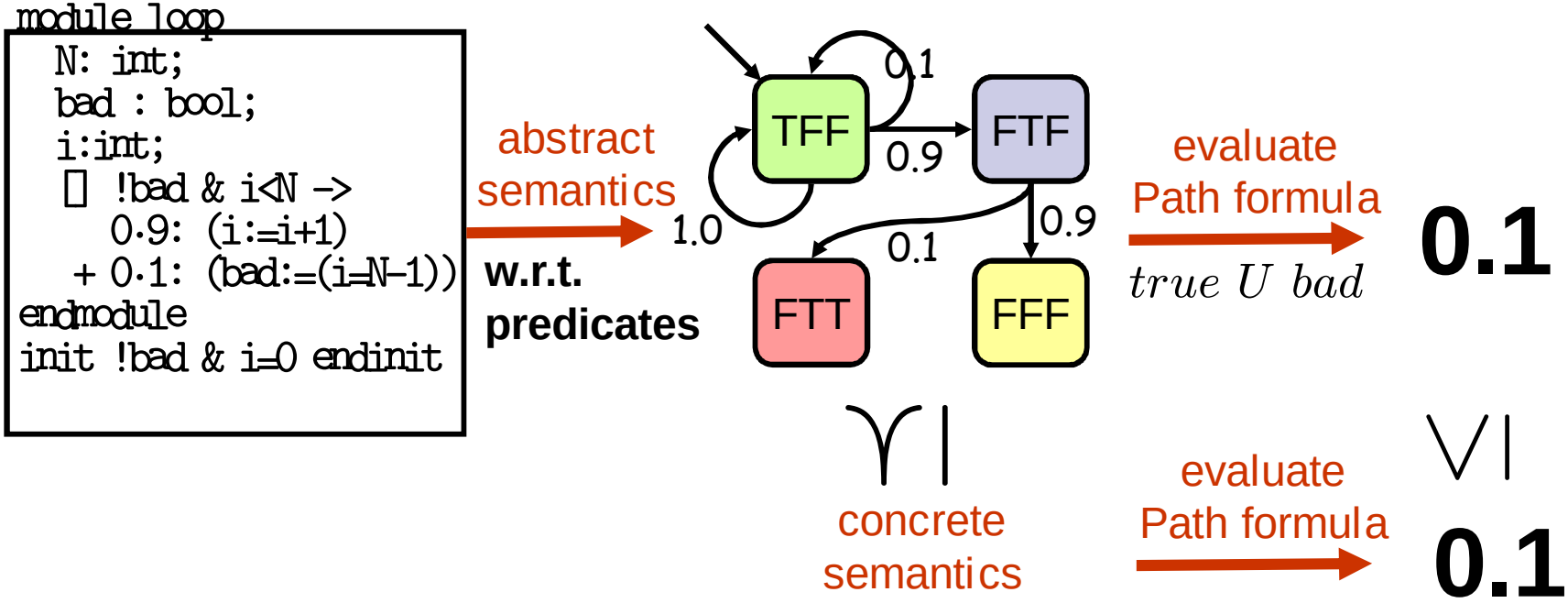
Previous Work vs Our Work

- Previous Work: **dÓArgenio, Kwiatkowska, de Alfaro, é**
- Our tool PASS (like SLAM, BLAST)
  - Abstract directly from program
  - **Donó compute concrete semantics** $\not\models \Phi$

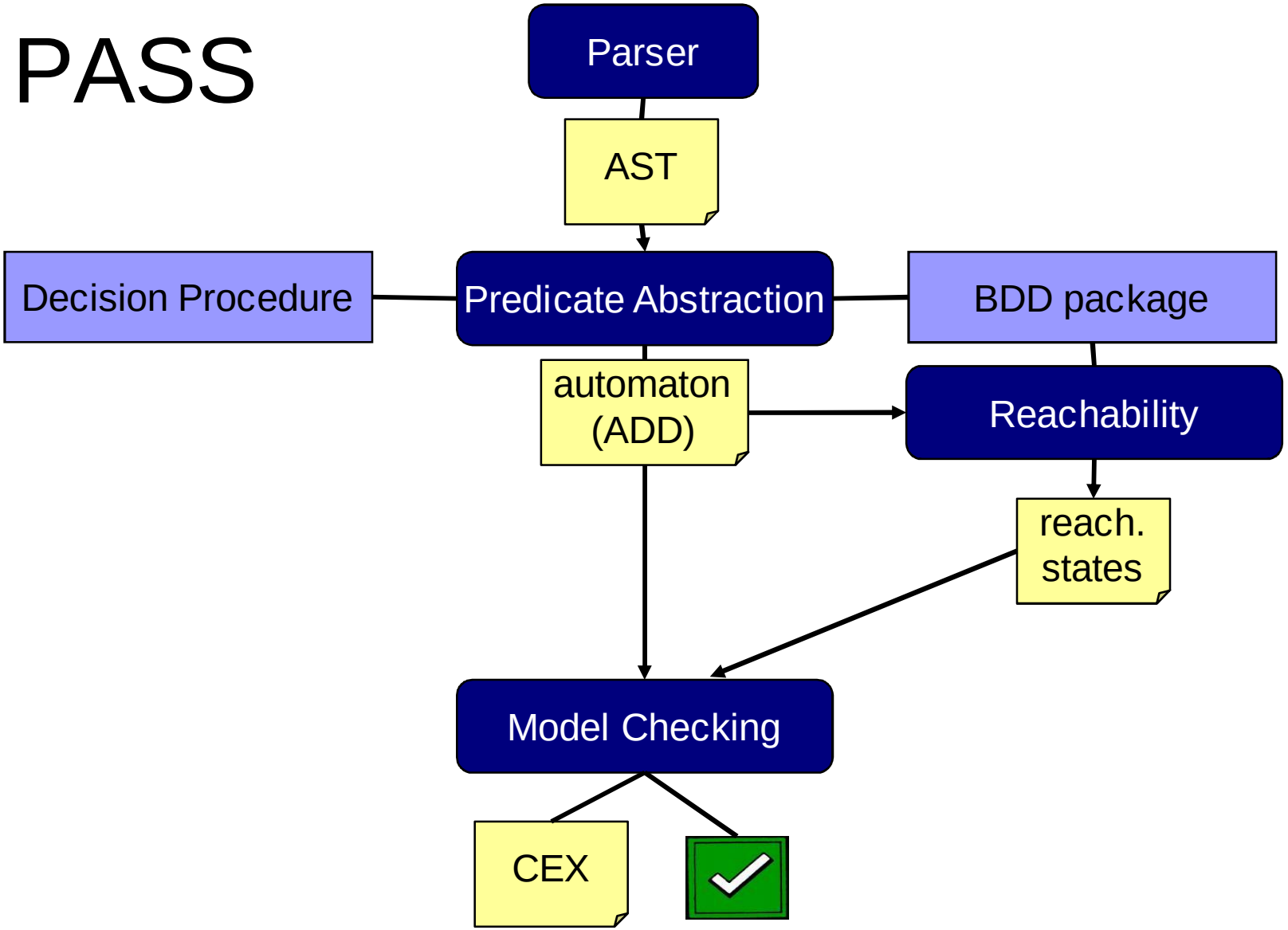


Abstraction

- **Abstract Probabilistic Automaton**
  - Soundness: Strong simulation preserves safe PCTL
  - Abstract automaton: get upper bound on Ăoriginalñprobability



PASS


Parser
AST
Decision Procedure
Predicate Abstraction
BDD package
automaton
(ADD)
Reachability
reach.
states
Model Checking
CEX

Wrap-up

- **Predicate abstraction for probabilistic models**
  - Language-level abstraction
  - Methods for efficient computation of abstract automaton
  - Abstraction based on **satisfiability modulo theory** solvers
- **Implemented in verification tool PASS**

http://depend.cs.uni-sb.de/pass