On the Probabilistic Symbolic Analysis of Programs

Antonio Filieri, Corina S. Pasareanu

Mateus Borges, Marcelo d'Amorin, Matt Dwyer, Jaco Geldenhuys,
Kasper Luckow, Willem Visser

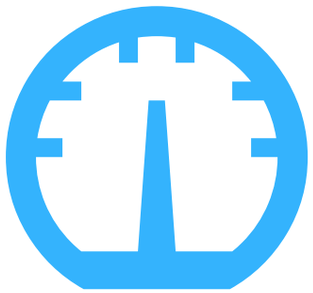
University of Stuttgart
Germany

Carnegie Mellon University
Silicon Valley

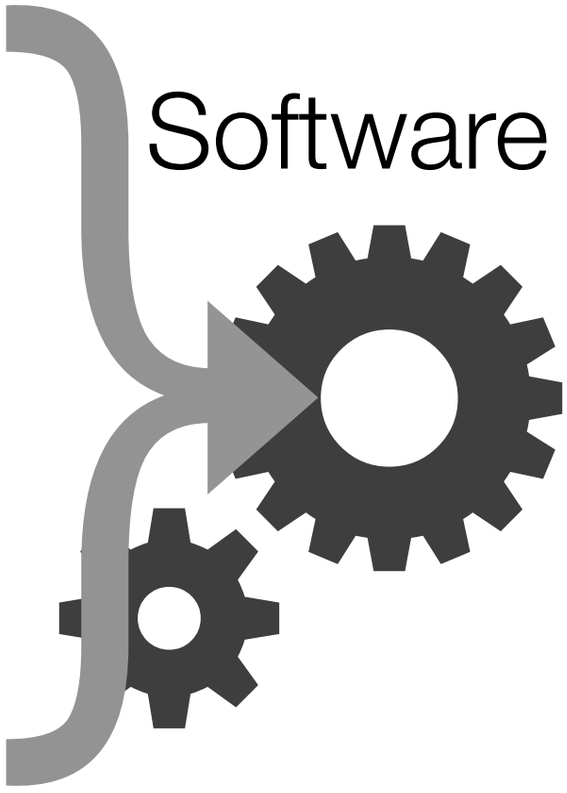
NASA Ames Research Center

```
public class OnBoardAbordExecutive {

  public void checkSafety(int pressure, int
  altitude, int spinSpeed){
    int discountedPressure = pressure - altitude/2;
    ...
    if(discountedPressure > 80 && spinSpeed>72){
      abort();
    }

    ...
    return;
}
...
```

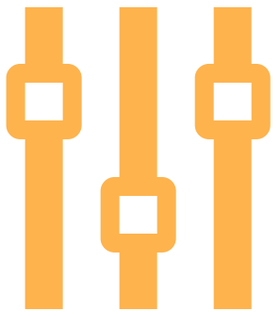
Sensors

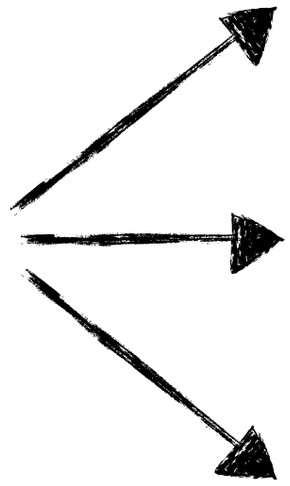


Software



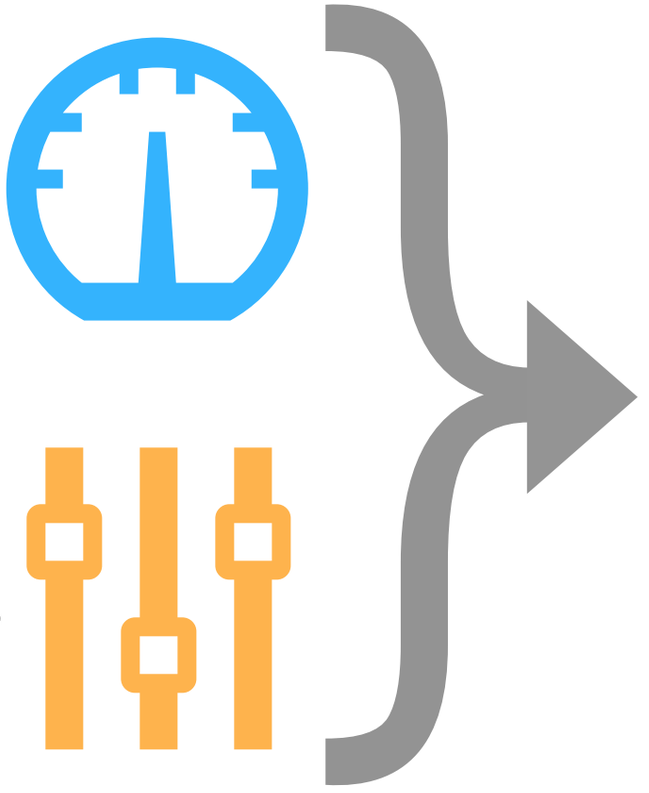
Commands



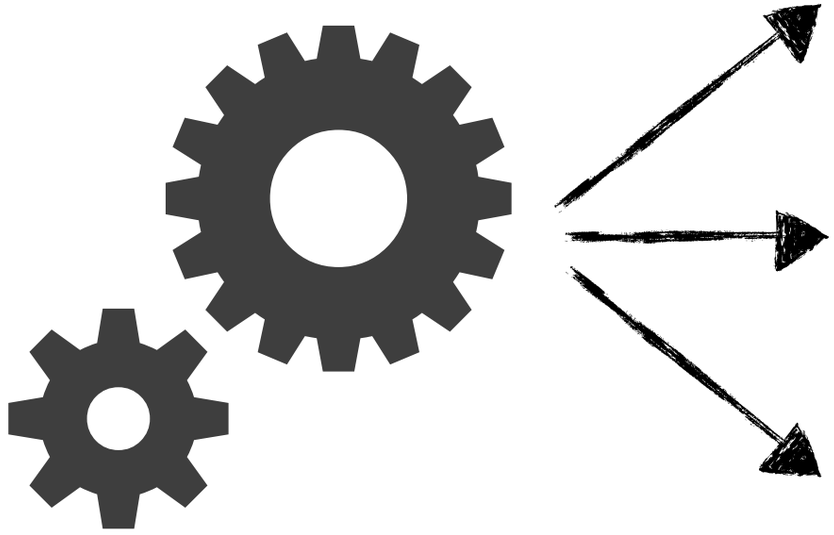


Sensors

Commands



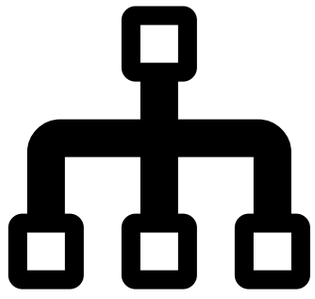
Software



Probability of

Probabilistic
Usage Profile

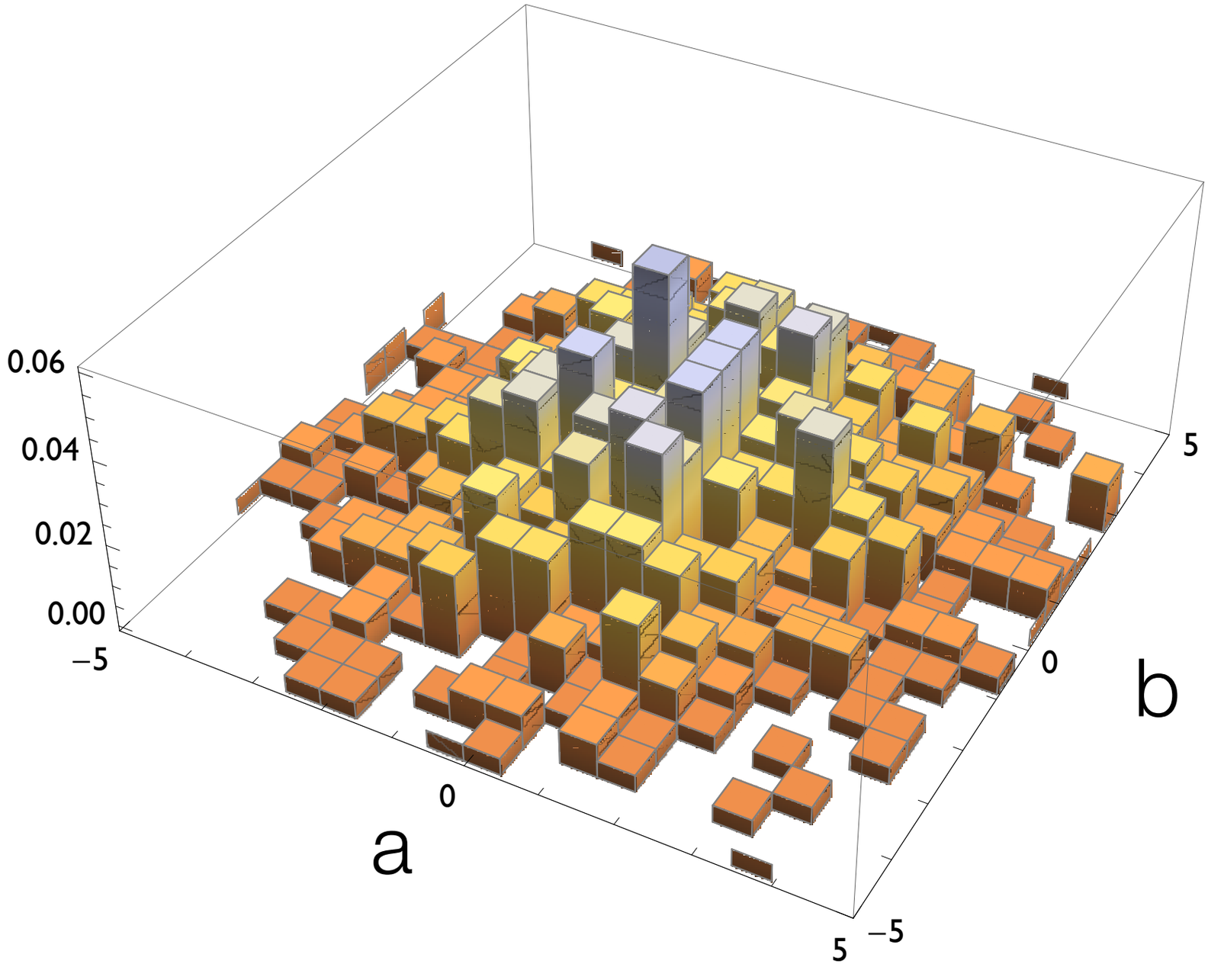
+

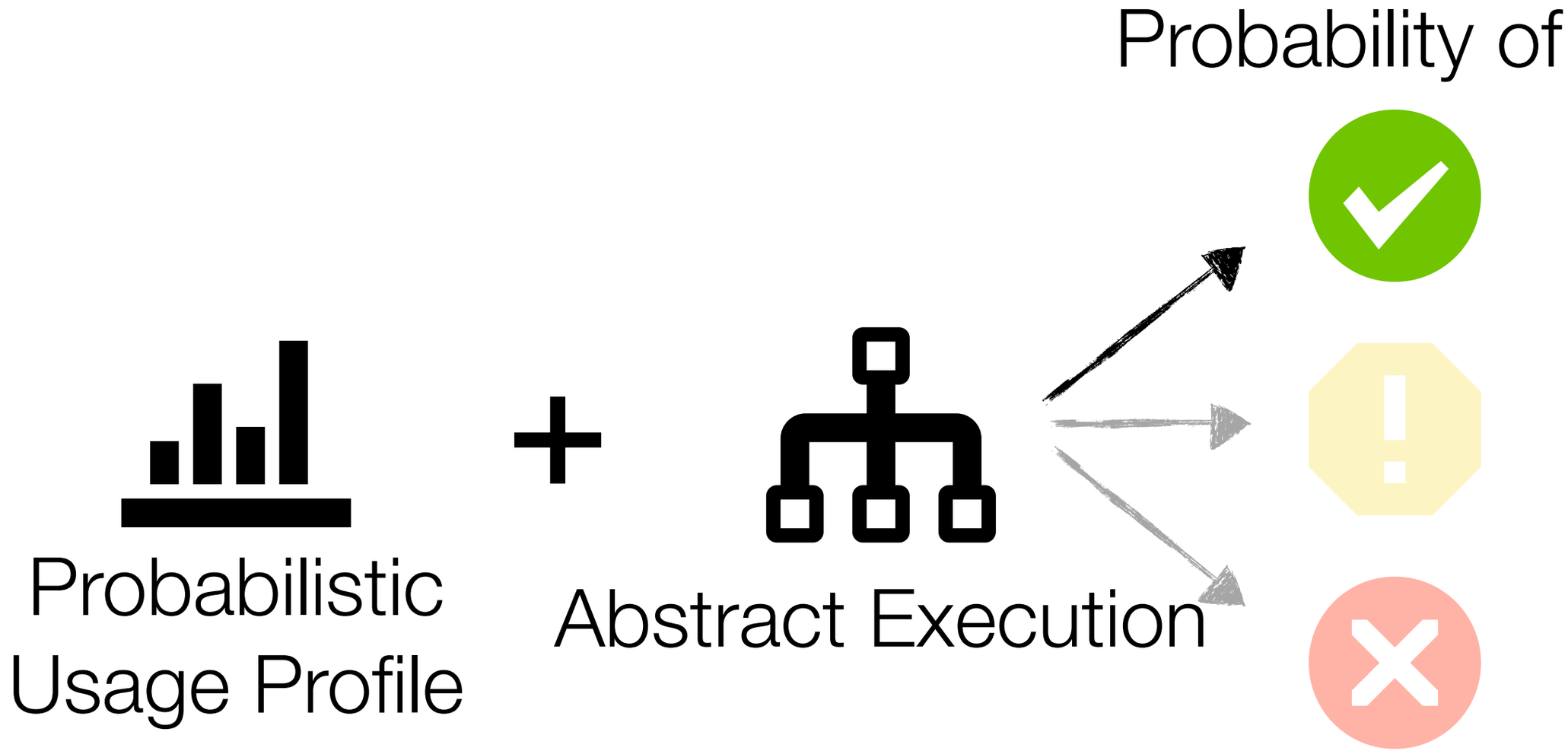


Abstract Execution

Probabilistic Usage Profile

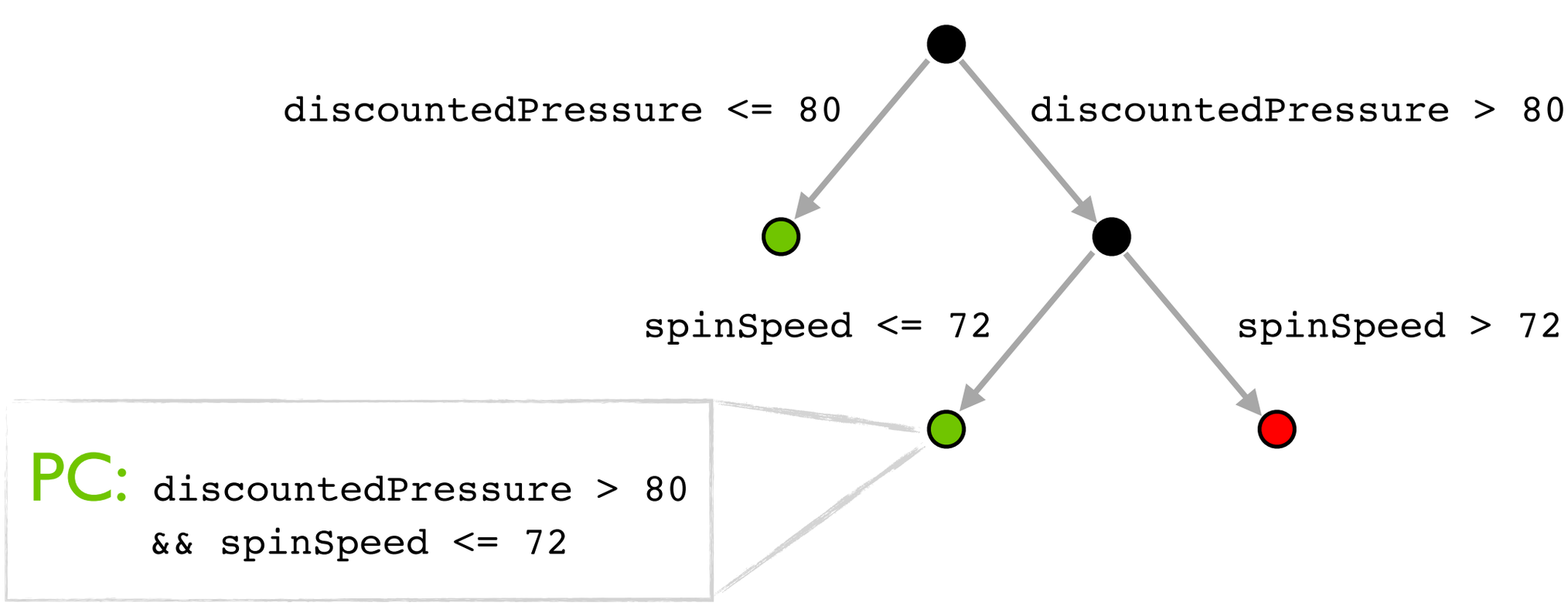
Arbitrarily accurate discretization



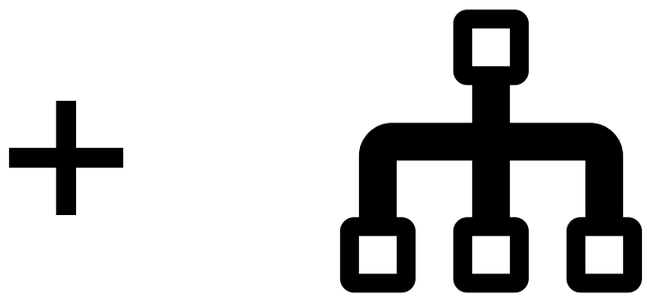

Probability of
Probabilistic
Usage Profile
+
Abstract Execution

Abstract Execution

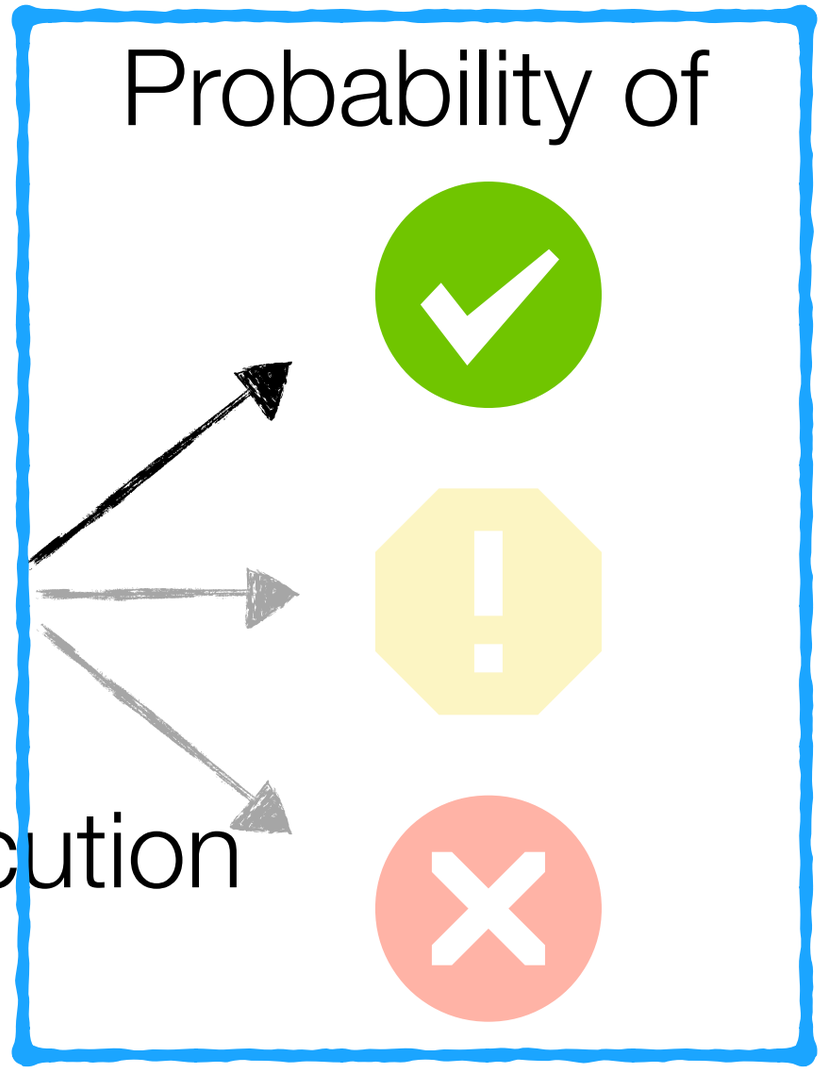
More precisely Symbolic Execution



Probabilistic
Usage Profile



Abstract Execution



Pr(PCs | UP)

…and the confidence on such result

Pr(PCs | UP)

Initial contribution [ICSE 2013]:

- General white-box methodology for finite domains using integer model counting, with explicit measure of confidence
- Handling linear integer constraints with polytopes analysis and our divide and conquer strategy
- Bounded execution for loops and recursion, multithreading
- Based on Korat for data structures

In the last year

- Dealing with floating-point numbers and non-linear constraints [PLDI 2014]
- Approximate incremental analysis [FSE2014]
- Synthesis of optimal schedulers for multithreading [ASE2014?]
- Improved support for data structures
- Parallelization

The boiling pot

- Nondeterminism
- Strings
- Dynamic discretization of continuous CDF
- Distribution-aware statistical methods
- Probabilistic loop invariants
- “Usage-coverage” criteria
- Errors and bug ranking (prioritization)
- Usage profile inference
- Automatic data-structures and code selection
- Quantitative information flow analysis [SPIN2014?]