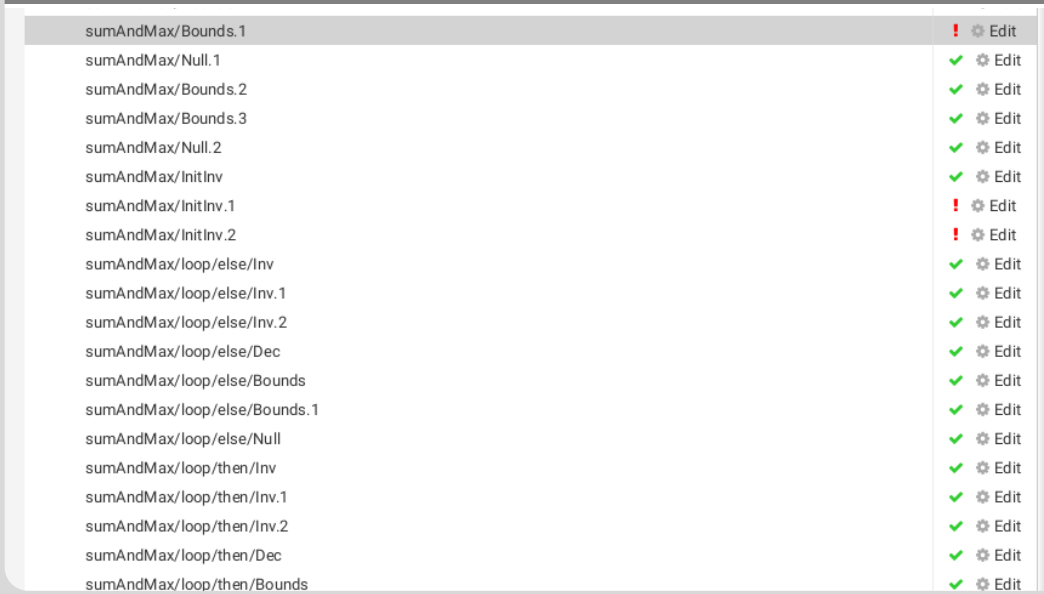
Karlsruhe Institute of Technology

Seamless Interactive Program Verification
Demo of AlgoVer

Sarah Grebing, Mattias Ulbrich, Jonas Klamroth

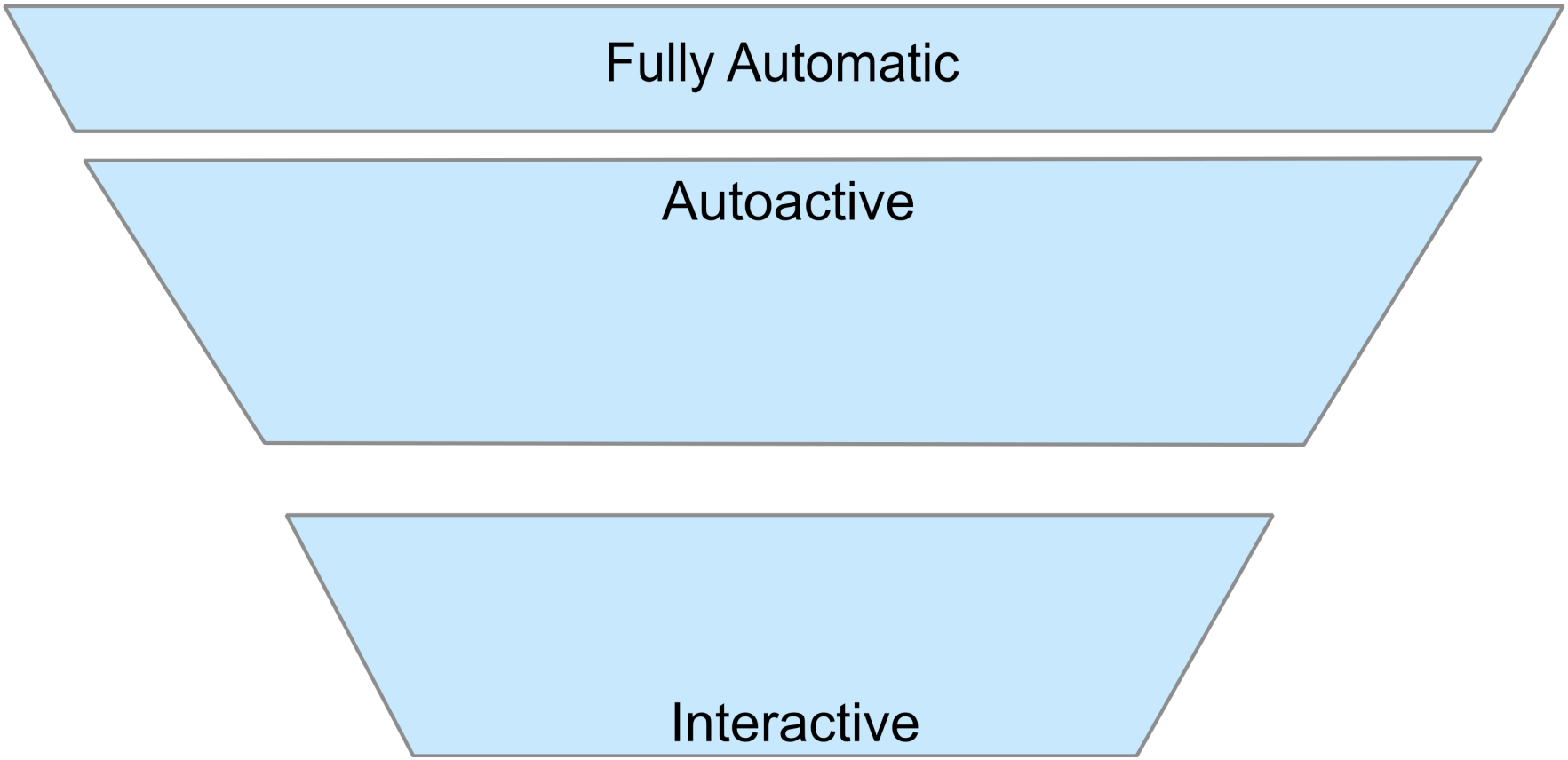
Institut für Theoretische Informatik, KIT



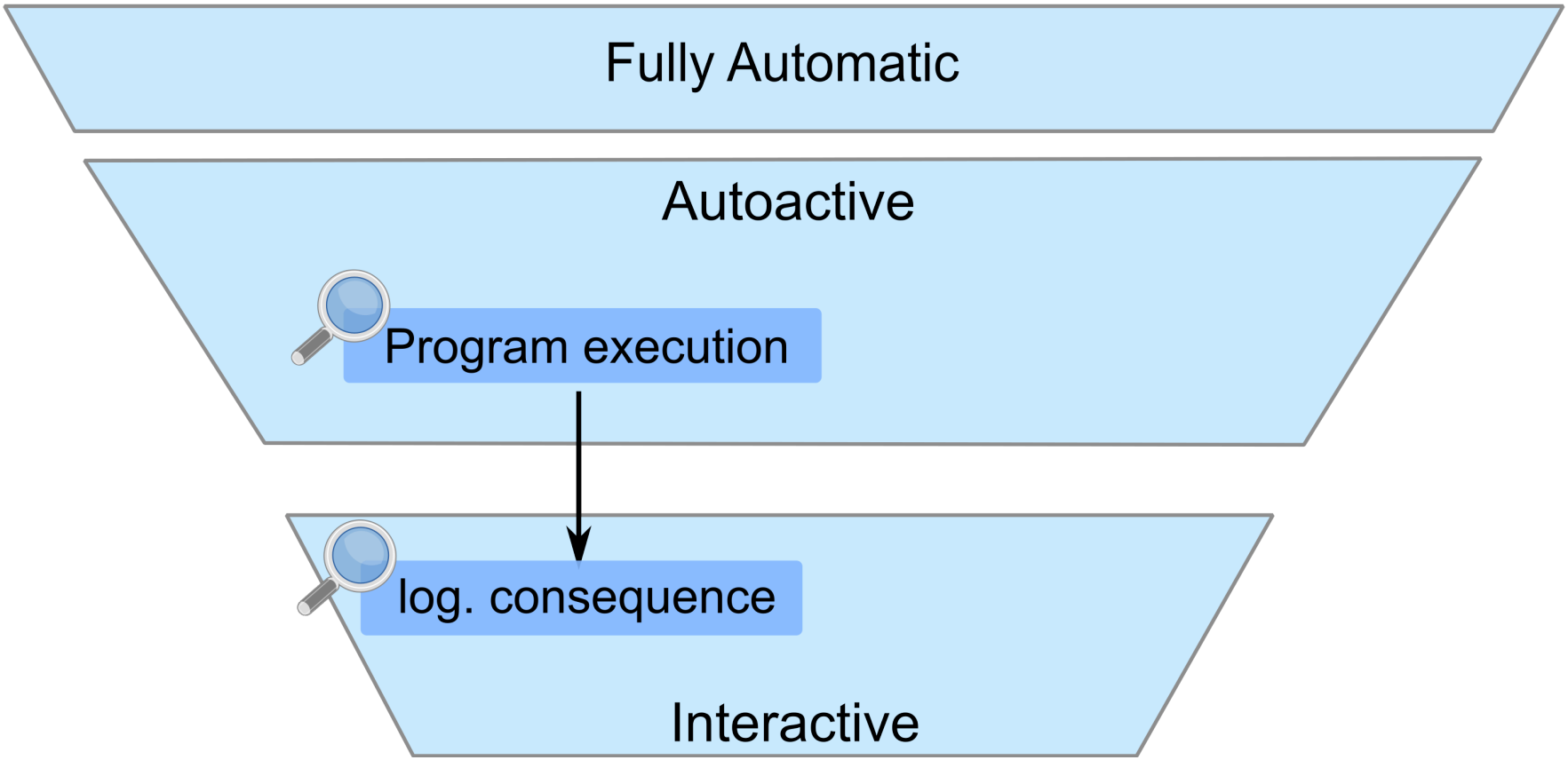

```
  sum := a[0];
  max := a[1];

  var i: int := 1;
  while (i < a.Length)
    invariant 0 <= i && i <= a.Length
    invariant forall k: int :: 0 <= k && k < i ==> a[k] <= max
    invariant i * max >= sum
    decreases a.Length - i
  {
    if (a[i] > max)
    {
      max := a[i];
    }
    sum := sum + a[i];
    i := i + 1;
  }
}
```

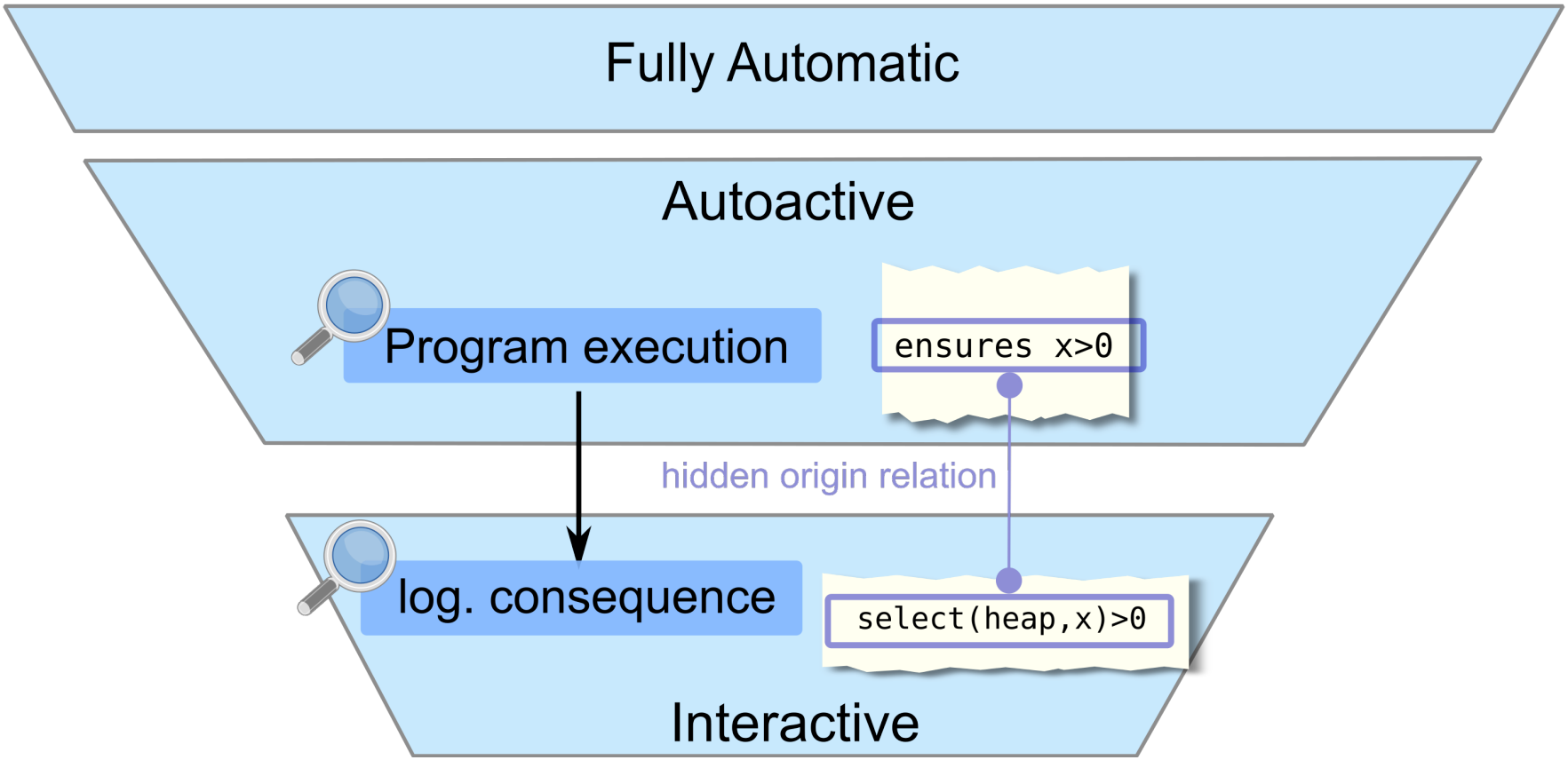
Interactive Program Verification



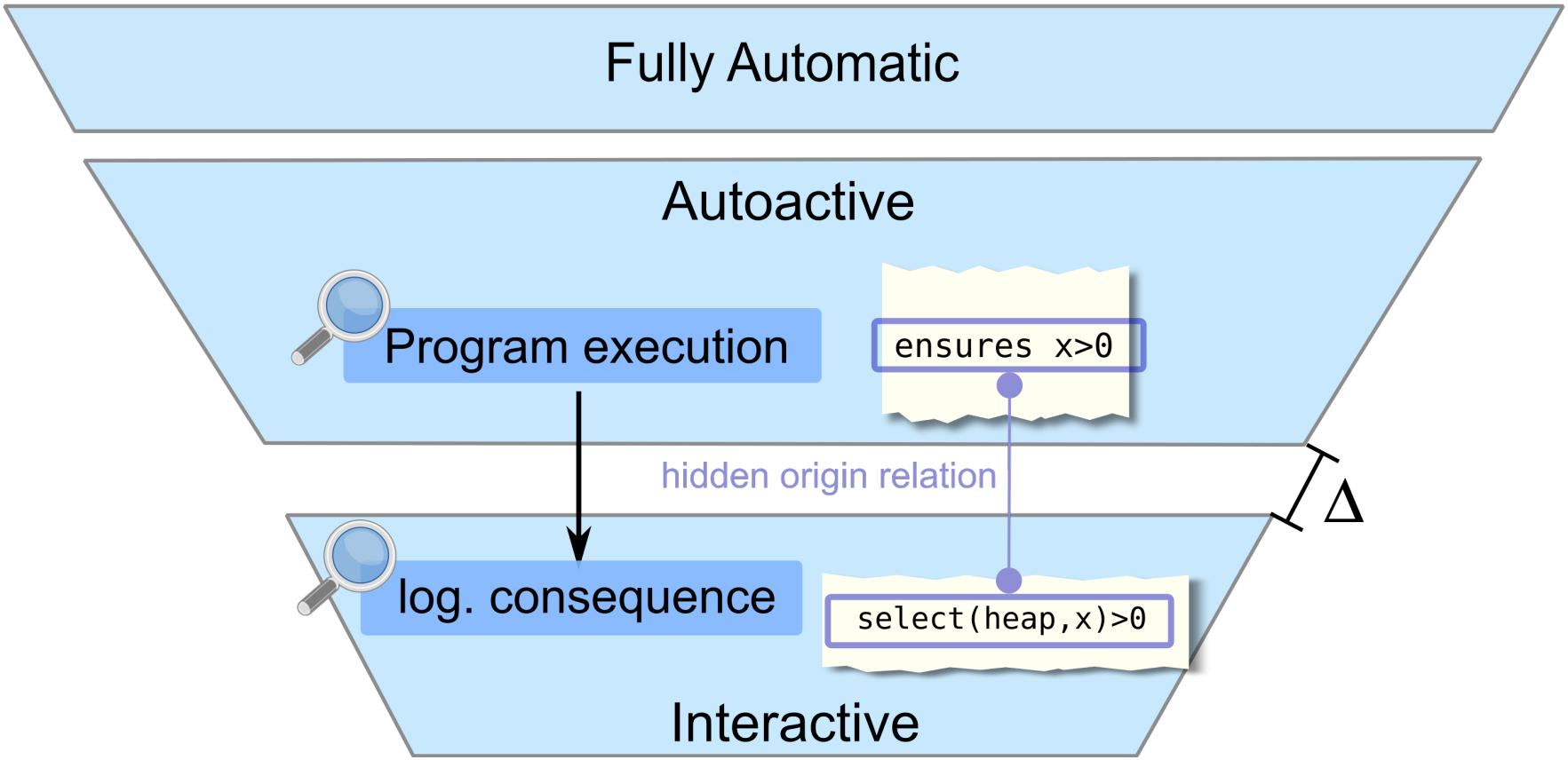
Interactive Program Verification



Interactive Program Verification



Interactive Program Verification



AlgoVer: Seamless Program Verification

Karlsruhe Institute of Technology

- Interactive program verification for Dafny
  - Symbolic execution (à la KeY)
  - Innovative interaction concepts
  - Calling z3
- Bridging the gap between code and proof

Karlsruhe Institute of Technology

Demo

Features And Future Work

Features:

- Inspection of different parts of the proof in individual views
- Seamless transition between different views
- Proof construction using
  - direct manipulation
  - script based
  - annotation based

Future Work:

- More rules and strategies
- Improved SMT-support
- Feedback/Interaction back to annotations in source code
- Evaluation on larger examples
- ...