

### Seamless Interactive Program Verification Demo of AlgoVer

Sarah Grebing, Mattias Ulbrich, Jonas Klamroth

```
Institut für Theoretische Informatik, KIT
                                                                                                                         sum := a101;
  sumAndMax/Bounds.1
                                                                                                                         max := a[1];
  sumAndMax/Null.1

✓ Ó Edit

                                                                                                                        var i: int := 1:
  sumAndMax/Bounds 2

✓ Ø Edit

                                                                                                                        while (i < a.Length)
                                                                                                                         invariant 0 <= i && i <= a.Length
  sumAndMax/Bounds.3

✓ Ö Fdit.

                                                                                                                         invariant forall k: int :: 0 <= k && k < i ==> a[k] <= max
  sumAndMax/Null 2

 O Edit

                                                                                                                          invariant i * max >= sum
  sumAndMax/InitInv

 O Edit

                                                                                                                   15
  sumAndMax/InitInv 1
                                                                                                       • O Edit
  sumAndMax/InitInv.2
                                                                                                       ! ○ Edit
                                                                                                                            max := a[i]:
  sumAndMax/loop/else/Inv

✓ ⊕ Edit

  sumAndMax/loop/else/Inv.1

✓ ⊕ Edit

                                                                                                                           sum := sum + a[i]:
  sumAndMax/loop/else/Inv.2

✓ © Edit

  sumAndMax/loop/else/Dec

✓ Ø Edit

  sumAndMax/loop/else/Bounds
                                                                                                       J IS Edit
  sumAndMax/loop/else/Bounds.1

✓ Ø Edit

  sumAndMax/loop/else/Null

✓ ○ Edit

✓ ○ Edit

  sumAndMax/loop/then/Inv

✓ ○ Edit

  sumAndMax/loop/then/lnv.1
  sumAndMax/loop/then/Inv.2

✓ ○ Edit

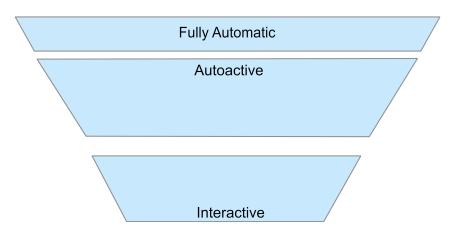
  sumAndMax/loop/then/Dec

✓ ⊕ Edit

  sumAndMax/loop/then/Bounds

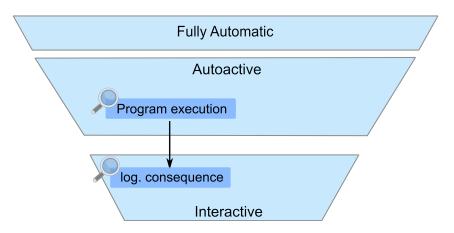
✓ Ø Edit
```





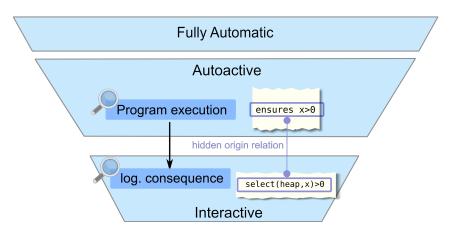








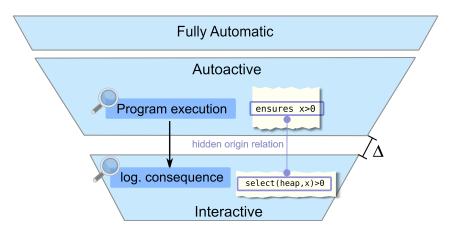




August 14, 2018Sarah Grebing, Mattias Ulbrich, Jonas Klamroth - Seamless Interactive Program Verification

Demo of AlgoVer





Institut für Theoretische Informatik, KIT

# **AlgoVer: Seamless Program Verification**



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

## Demo



# 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
- **...**

