Symbolic Verification via Program Transformation

Henrich Lauko

Masaryk University

Brno, Czech Republic

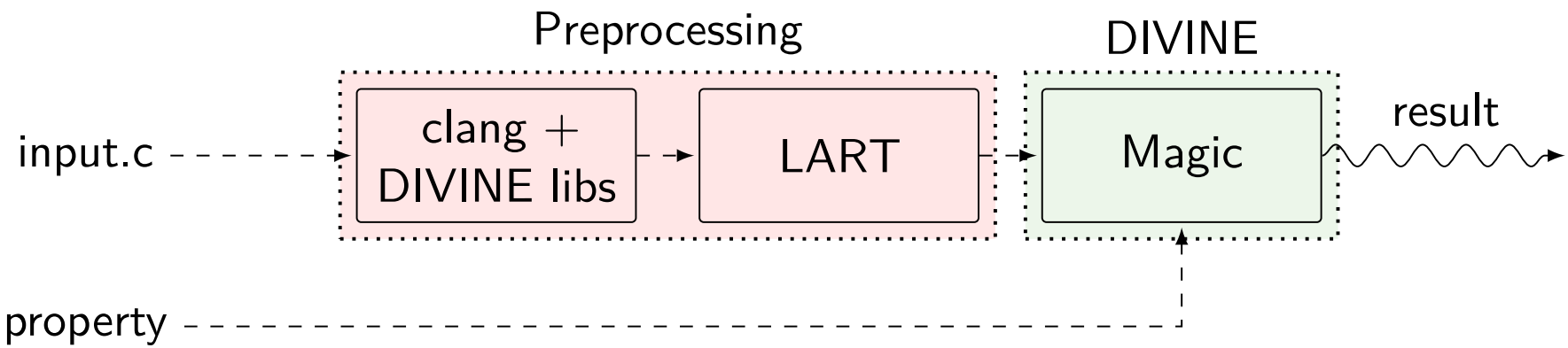
10th May 2018

Topic Recapitulation

- verification of programs with inputs

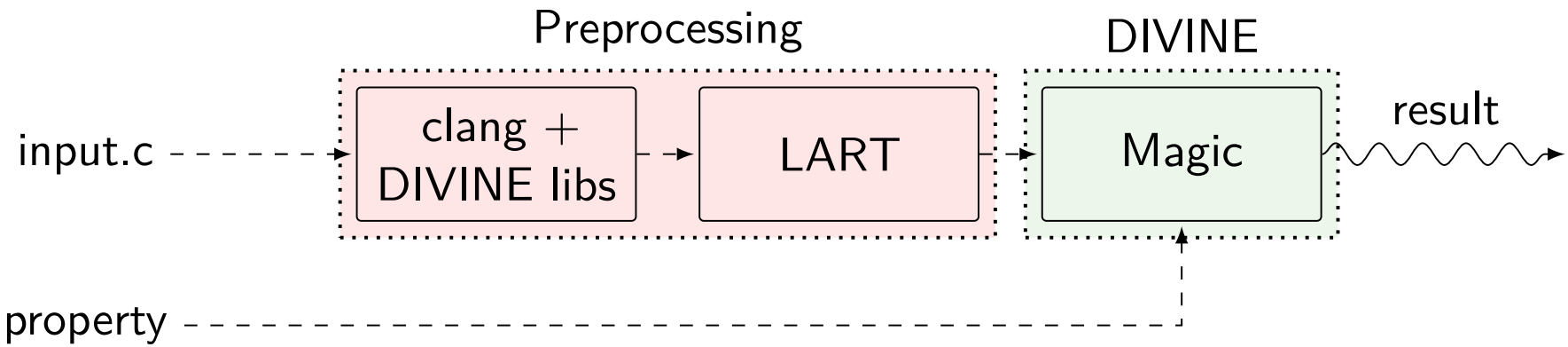
Topic Recapitulation

- verification of programs with inputs
- transform the program to manipulate symbolic representation instead of concrete inputs



Topic Recapitulation

- verification of programs with inputs
- transform the program to manipulate symbolic representation instead of concrete inputs



- **Diploma thesis:** prototype that can abstract values on stack

Current Status

1. **new concept of transformation:**

Current Status

1. **new concept of transformation:**

   - enables abstraction of data on the heap

Current Status

1. **new concept of transformation:**

- enables abstraction of data on the heap
- added support of arrays with abstract values

Current Status

1. **new concept of transformation:**

- enables abstraction of data on the heap
- added support of arrays with abstract values
- get rid of necessity to compute shapes of data structures
  - enables arbitrary structure with abstract data

Current Status

1. **new concept of transformation:**
   - enables abstraction of data on the heap
   - added support of arrays with abstract values
   - get rid of necessity to compute shapes of data structures
     - enables arbitrary structure with abstract data
2. **polishing of code:**
   - simplification of whole process (from 6000 loc. to 2500 loc.)

Current Status

1. **new concept of transformation:**
   - enables abstraction of data on the heap
   - added support of arrays with abstract values
   - get rid of necessity to compute shapes of data structures
     - enables arbitrary structure with abstract data
2. **polishing of code:**
   - simplification of whole process (from 6000 loc. to 2500 loc.)
3. **finishing paper resubmition**
   - evaluation should now cover bigger portion of SV-COMP
   - TODO preliminary results

Plans for the rest of 2018

May:

- evaluation + paper submission

Plans for the rest of 2018

May:

- evaluation + paper submission

June – September

- string abstraction in cooperation with italian Ph.D. student

Plans for the rest of 2018

May:

- evaluation + paper submission

June – September

- string abstraction in cooperation with italian Ph.D. student
- further work on memory abstractions

Plans for the rest of 2018

May:

- evaluation + paper submission

June – September

- string abstraction in cooperation with italian Ph.D. student
- further work on memory abstractions
- trip to Aachen to familiarize with local team before Erasmus

Plans for the rest of 2018

May:

- evaluation + paper submission

June – September

- string abstraction in cooperation with italian Ph.D. student
- further work on memory abstractions
- trip to Aachen to familiarize with local team before Erasmus
- summer school on automated reasoning (Manchester)

Plans for the rest of 2018

May:

- evaluation + paper submission

June – September

- string abstraction in cooperation with italian Ph.D. student
- further work on memory abstractions
- trip to Aachen to familiarize with local team before Erasmus
- summer school on automated reasoning (Manchester)

October – December

- Erasmus at Aachen

Plans for the rest of 2018

May:

- evaluation + paper submission

June – September

- string abstraction in cooperation with italian Ph.D. student
- further work on memory abstractions
- trip to Aachen to familiarize with local team before Erasmus
- summer school on automated reasoning (Manchester)

October – December

- Erasmus at Aachen
- work on utilization of SMT solving in verification