Implementing Termination Analysis using Configurable Software Verification

Sebastian Ott

Termination

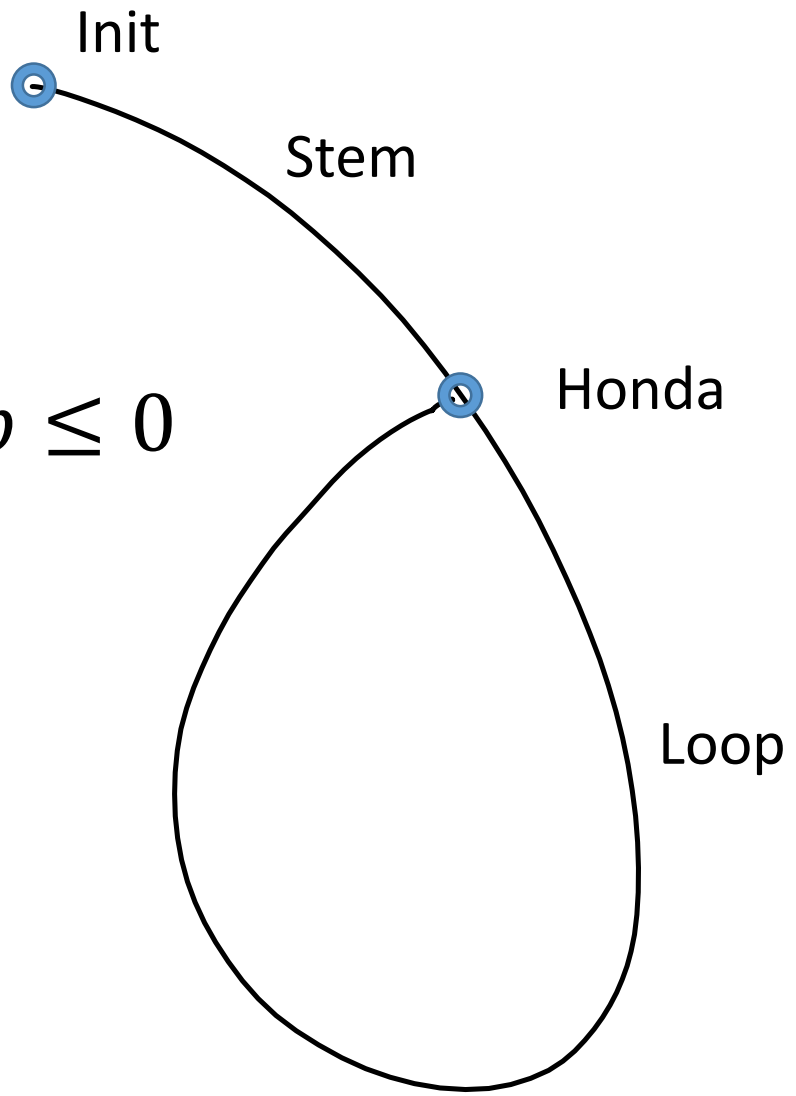
- No infinite execution
- Liveness property
- Important property of programs:
  - partial correctness $\wedge$ termination $\Rightarrow$ total correctness
- Undecidable in general

LassoRanker

- Java library from Ultimate Automizer
- Synthesis of
  - Termination arguments
  - Non-termination arguments
- Template based approach
- SMT solver as back-end
- Lasso as input

Lasso

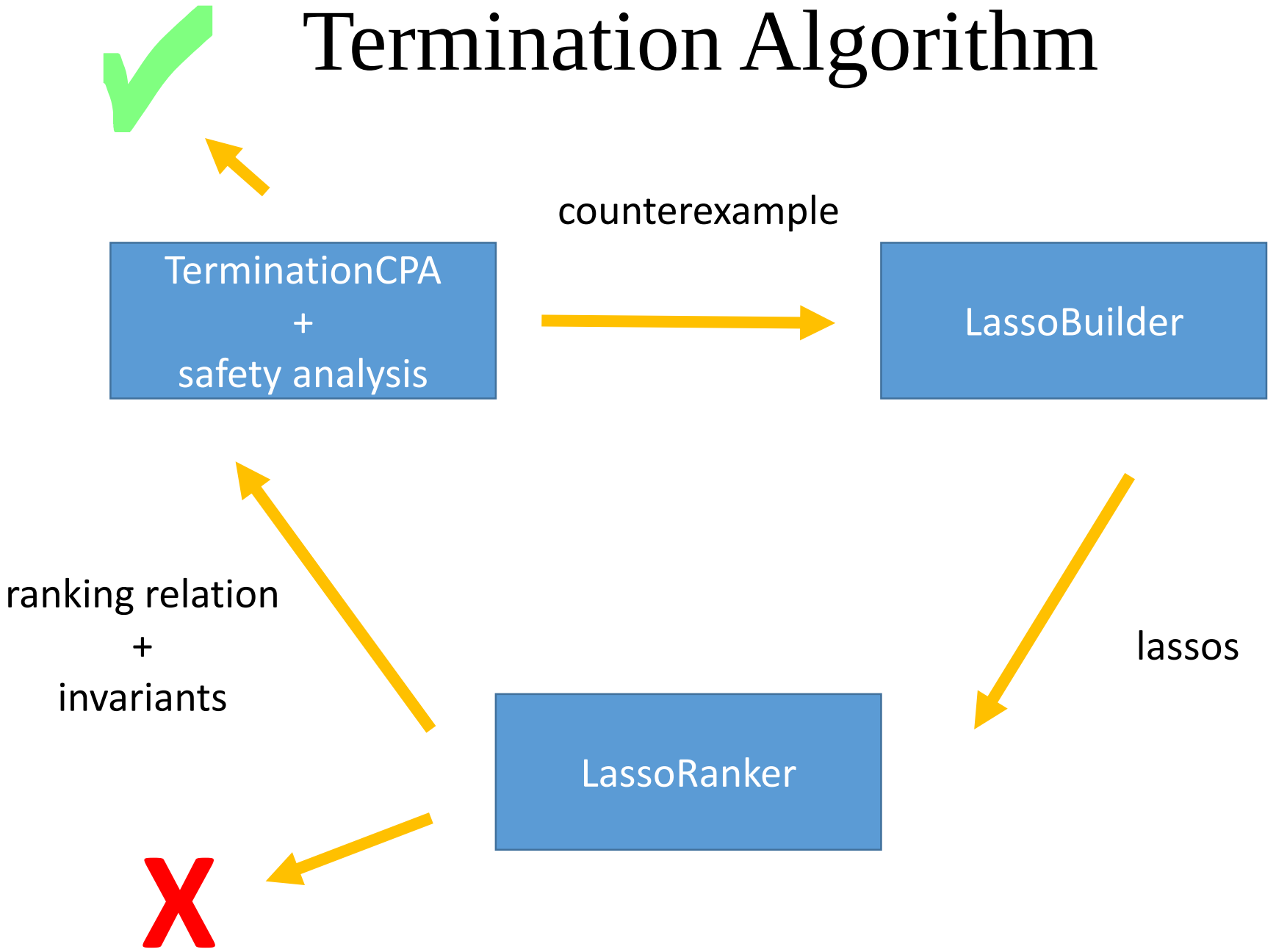
- Simple loop program
- $(x', x) \in Loop \Leftrightarrow A \begin{pmatrix} x' \\ x \end{pmatrix} + b \leq 0$
- SMT formula in DNF



Composition of Termination Arguments

- $Loop$ is well-founded if $Loop \subseteq T$ and T is well-founded.
- Disjunctively well-founded relation $R \subseteq T_1 \cup T_2$ ...
- R is well-founded if its transitive hull is disjunctively well-founded.

Termination Algorithm



TerminationCPA

- Searches for potentially non-terminating lassos
- Separation of stem and loop
- Program instrumentation at Honda
  - Stem-loop-transition: x‘ = x; y’ = y;
  - Loop head --[! ranking relation] -> error location
- WrapperCPA
- ARGCPA – TerminationCPA – CompositeCPA

Restrictions and Challenges

- No support for recursion
- Unbounded arrays
- Encoding of termination arguments
  - Linear combination of pointers
  - Array cells: $a'[i] > a[i] \wedge a'[i] > 0$
- Number of disjunctions in lasso formulas
  - Pointer
  - $a \mathrel{!}= b \rightarrow (a < b) \vee (a > b)$

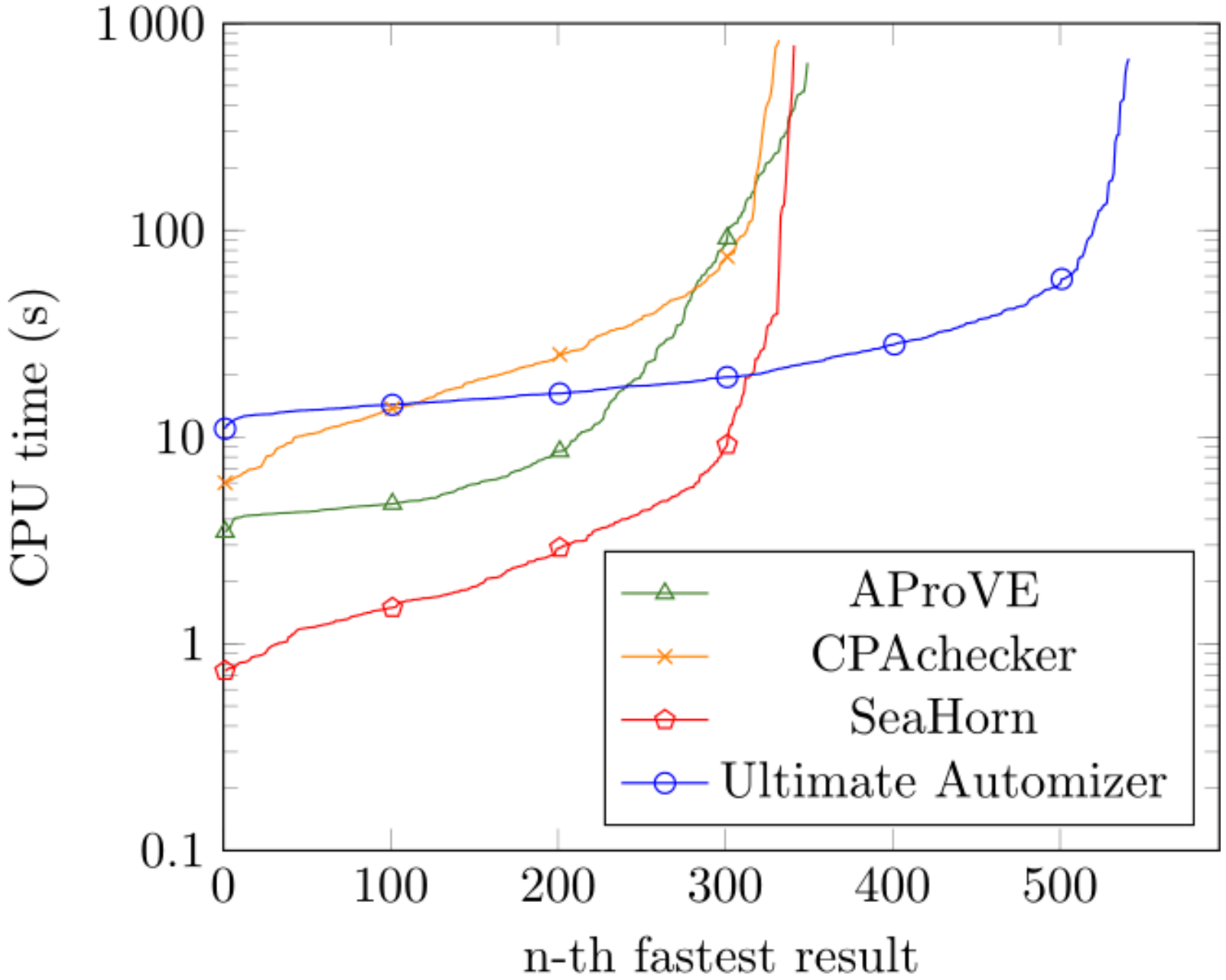
Evaluation

- Termination Algorithm + Predicate Analysis
- Participants of SV-COMP 2016
  - AProVE
  - SeaHorn
  - Ultimate Automizer
- 733 loop programs
- Limitations
  - 2 CPU cores
  - 900 s CPU time
  - 15 GB memory

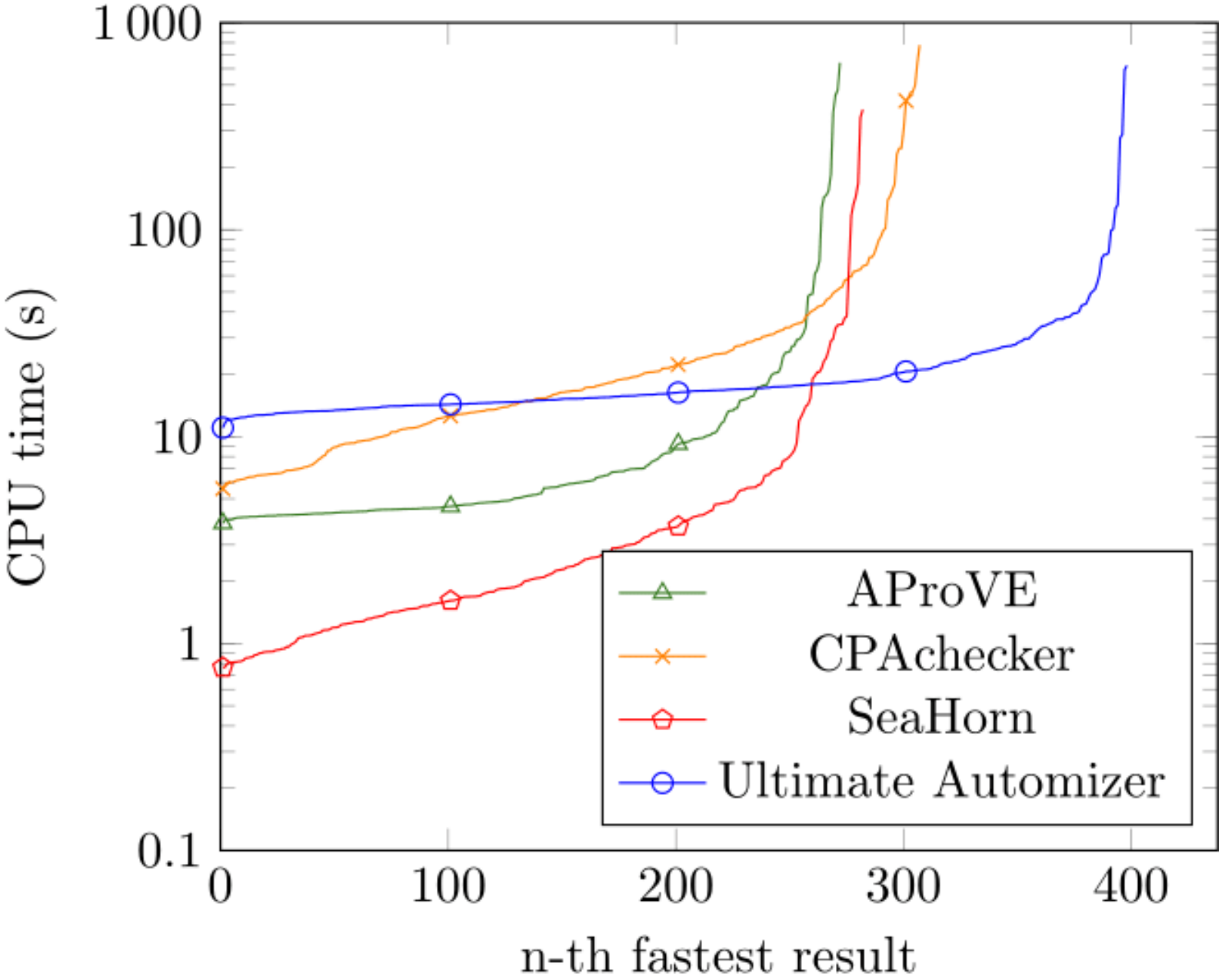
Evaluation

	AProVE	CPAchecker	SeaHorn	Ultimate Automizer
TRUE (569)	278	272	259	430
FALSE (136)	71	60	82	111
incorrect results	3	1	46	0
Ø CPU time	409 s	339 s	170 s	134 s
Ø memory	2870 MB	1600 MB	64,8 MB	1150 MB
Ø CPU time (correct results)	45,8 s	45,6 s	12,7 s	33,1 s
Ø memory (correct results)	1300 MB	596 MB	40,0 MB	528 MB

Evaluation


1 000
100
10
1
0.1
CPU time (s)
0
100
200
300
400
500
n-th fastest result
AProVE
CPAchecker
SeaHorn
Ultimate Automizer

Evaluation (without pointers)



Future Work

- More types of termination arguments
- Other tool for construction of (non-)termination arguments
- Better support of arrays
- Counterexample check
- Validation of witnesses

Conclusion

- Termination analysis in CPAchecker
- Based on the CPA concept
- Good result on programs without pointers
- Construction of lassos is inefficient for pointers

Questions?