Goblint Validator

Correctness Witness Validation by Abstract Interpretation

Simmo Saan[1(✉)] Julian Erhard[2,3] Michael Schwarz[2]
Stanimir Bozhilov[2] Karoliine Holter[1] Sarah Tilscher[2,3]
Vesal Vojdani[1] Helmut Seidl[2]

[1]University of Tartu, Tartu, Estonia
simmo.saan@ut.ee

[2]Technische Universität München, Garching, Germany

[3]Ludwig-Maximilians-Universität München, Munich, Germany

TACAS 2024

Goblint (Validator)

Goblint

- Static analyzer for C programs
- Specializes in concurrency
- Based on abstract interpretation
- *Sound*
- Implemented in OCaml

Goblint Validator

- Extension of Goblint
- YAML **correctness** witnesses
  - `location_invariant`
  - `loop_invariant`
- Validation track results
  - 3rd in MemSafety
  - 3rd in NoOverflows
  - 2nd in SoftwareSystems
  - **3rd in Overall**

Validation approach

Analysis *Unassume* witness invariants for speedup [VMCAI 2024]

- $\{\mathtt{x} \mapsto [0, \infty]\} \underset{\text{unassume}(\mathtt{x} \geq 0)}{\overset{\text{assume}(\mathtt{x}=0)}{\rightleftharpoons}} \{\mathtt{x} \mapsto [0, 0]\}$
- Faster fixpoint convergence
- Can also make analysis more precise

Post-processing Check witness invariants for correctness

Strengths

Generic: works in *all* SV-COMP categories

Weaknesses

Over-approximation: can only *confirm* correctness witnesses

Validation approach

Analysis *Unassume* witness invariants for speedup [VMCAI 2024]

- $\{\mathtt{x} \mapsto [0, \infty]\} \underset{\text{unassume}(\mathtt{x} \geq 0)}{\overset{\text{assume}(\mathtt{x}=0)}{\rightleftharpoons}} \{\mathtt{x} \mapsto [0, 0]\}$
- Faster fixpoint convergence
- Can also make analysis more precise

Post-processing Check witness invariants for correctness

Strengths

Generic: works in *all* SV-COMP categories

Weaknesses

Over-approximation: can only *confirm* correctness witnesses

Validation approach

Analysis *Unassume* witness invariants for speedup [VMCAI 2024]

- $\{\mathtt{x} \mapsto [0, \infty]\} \underset{\text{unassume}(\mathtt{x} \geq 0)}{\overset{\text{assume}(\mathtt{x}=0)}{\rightleftharpoons}} \{\mathtt{x} \mapsto [0, 0]\}$
- Faster fixpoint convergence
- Can also make analysis more precise

Post-processing Check witness invariants for correctness

Strengths

Generic: works in *all* SV-COMP categories

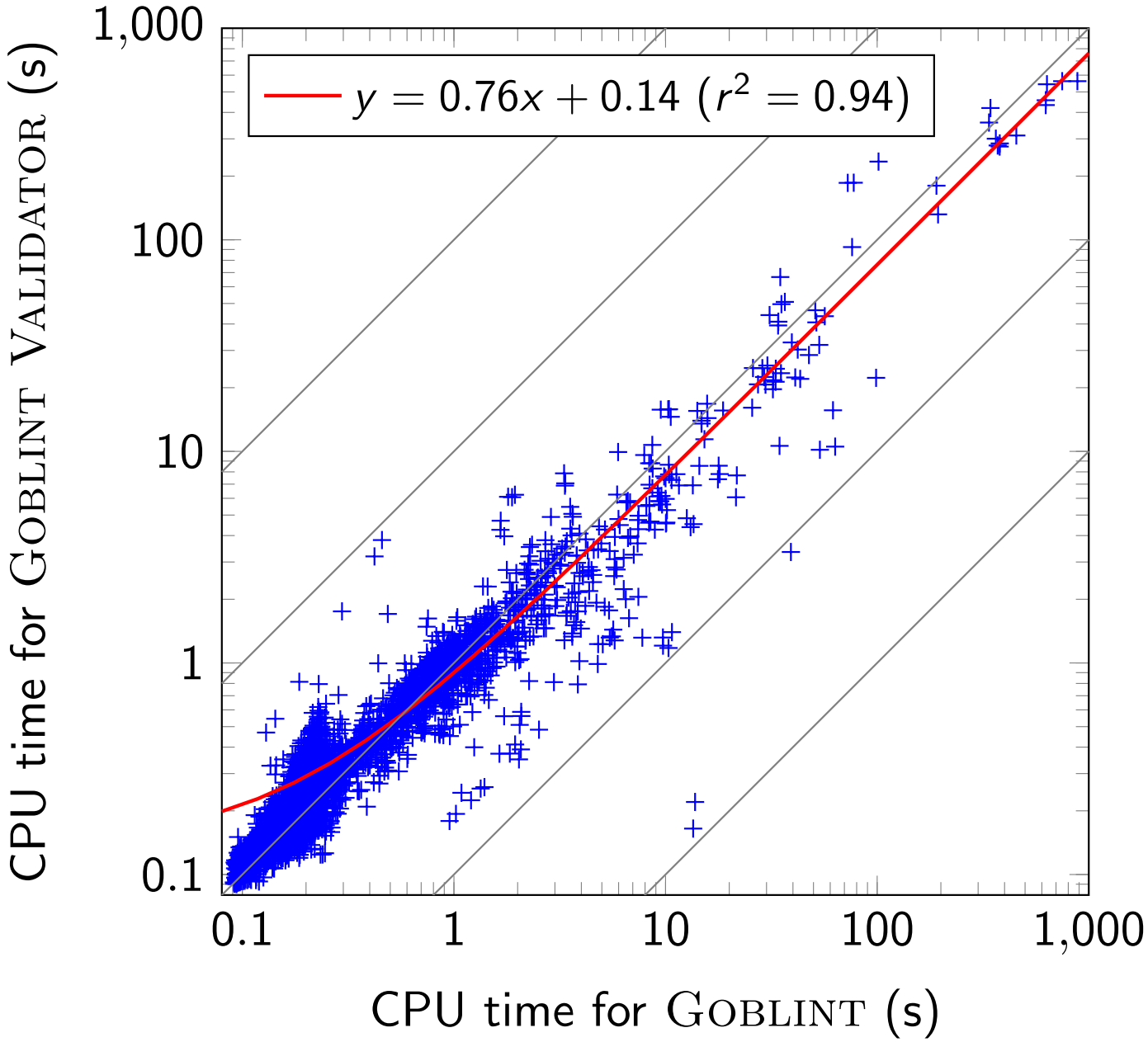
Weaknesses

Over-approximation: can only *confirm* correctness witnesses

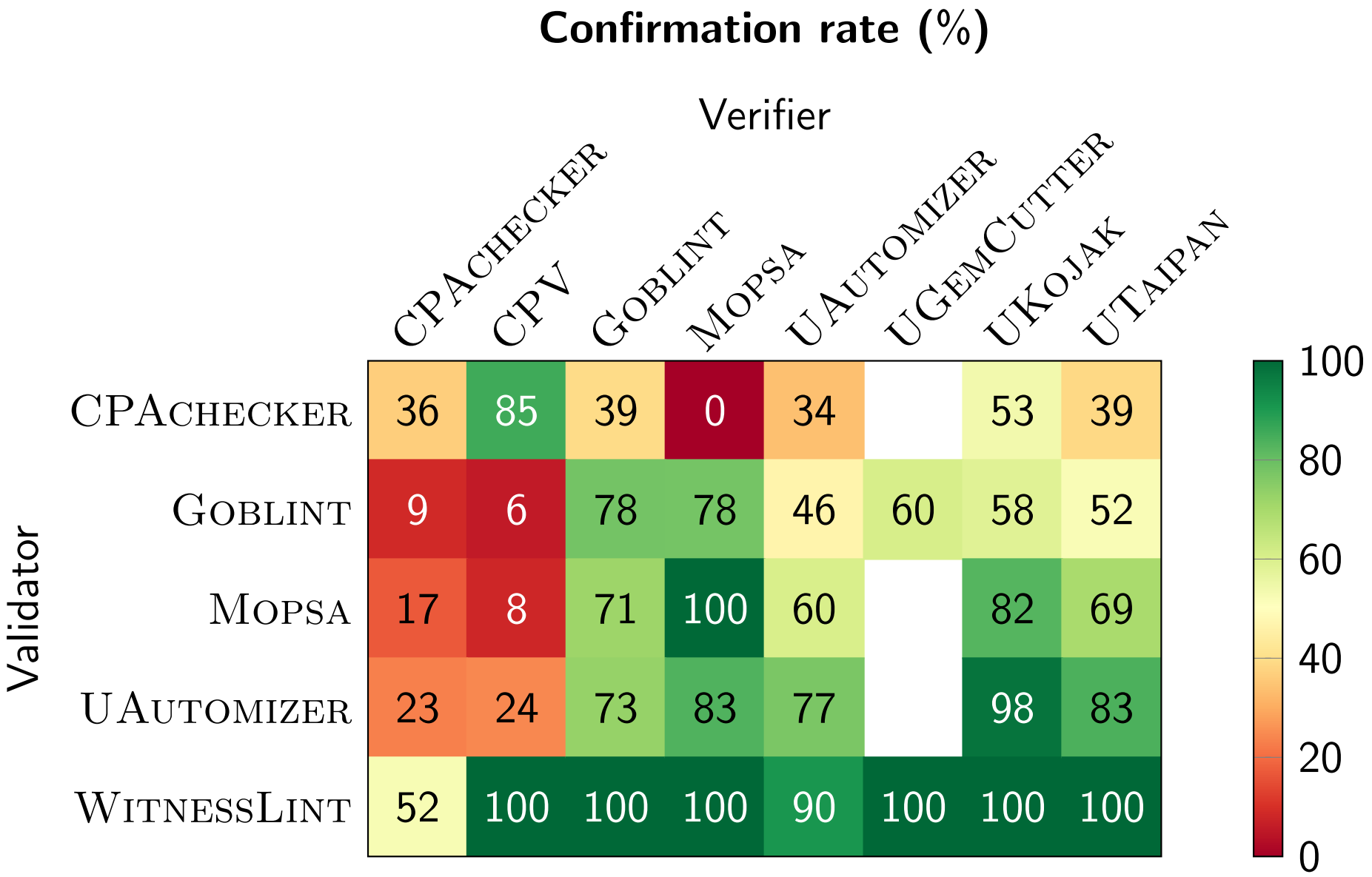
Same-framework consistency

Property	Correct tasks	GOBLINT verified	GOBLINT VALIDATOR Confirmed		GOBLINT VALIDATOR Unconfirmed
unreach-call	11,351	1,894	1,064	(56%)	830
no-overflow	5,562	3,932	3,416	(87%)	516
termination	1,536	619	297	(48%)	322
no-data-race	781	695	510	(73%)	185
valid-memsafety	2,796	1,963	1,801	(92%)	162
valid-memcleanup	2	0	–		–
Total	22,028	9,103	7,088	(78%)	2,015

Content-effort dependence



Cross-framework validation



Further reading

Saan, S., Erhard, J., Schwarz, M., Bozhilov, S., Holter, K., Tilscher, S., Vojdani, V., Seidl, H.
GOBLINT VALIDATOR: Correctness Witness Validation by Abstract Interpretation
In: TACAS 2024. pp. 335–340. Springer (2024).
DOI: https://doi.org/10.1007/978-3-031-57256-2_17

Saan, S., Schwarz, M., Erhard, J., Seidl, H., Tilscher, S., Vojdani, V.
Correctness Witness Validation by Abstract Interpretation
In: VMCAI 2024. pp. 74–97. Springer (2024).
DOI: https://doi.org/10.1007/978-3-031-50524-9_4

https://goblint.in.tum.de

https://github.com/goblint/analyzer