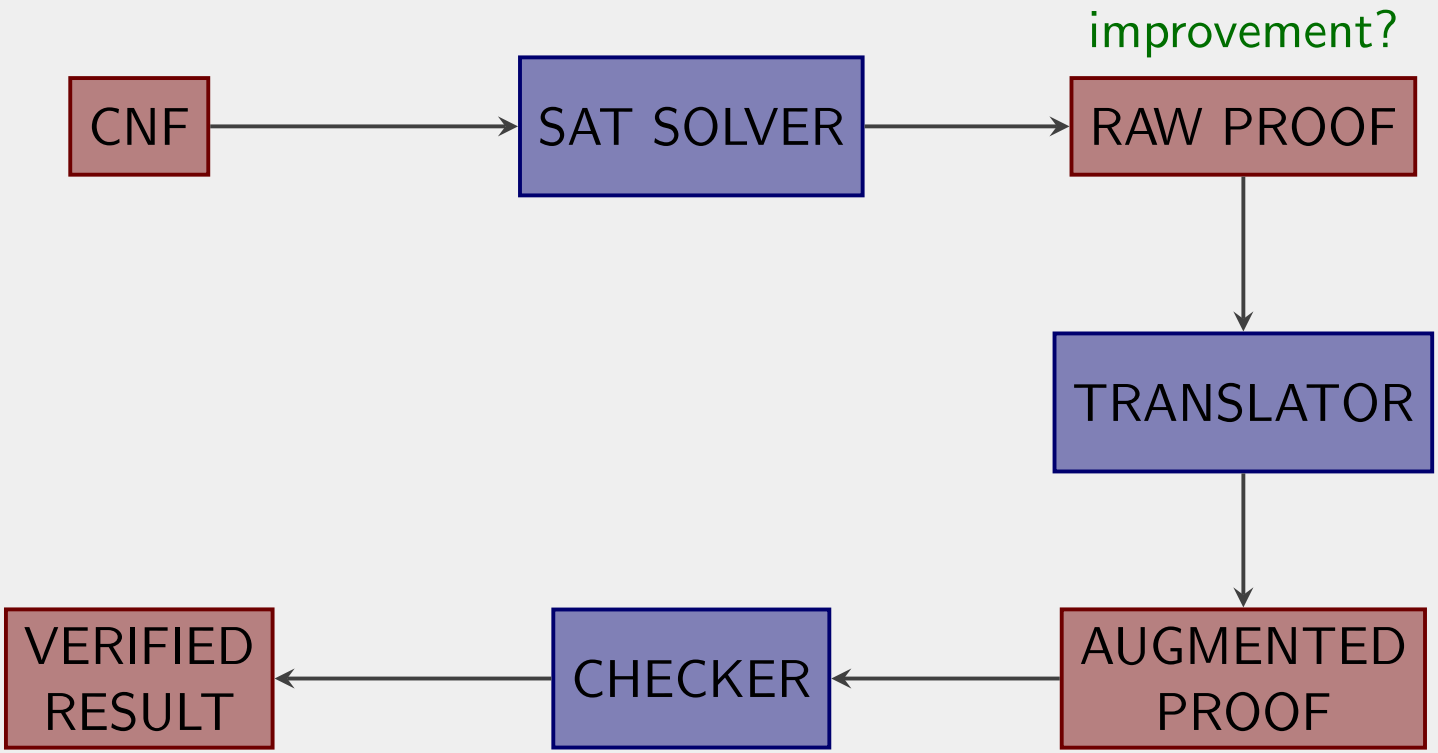
Efficient Proof Checking

implementing LRAT proofs in CaDiCaL

Florian Pollitt

March 23, 2023

What are we doing



Motivation

- reliable verifiable results
- proof certificates in the SAT competition
- real world applications
  - computer-aided proofs [KL15]
  - verifiying safety properties of computer hardware [Bie+99]
- developing SAT solvers

Proof Formats

- three different proof systems:
  - state of the art: DRAT [Heu16]
  - format with fast verified checkers: LRAT [Cru+17]
  - flexible proof format: FRAT [BCH22]

Comparing proof Formats

DIMACS

```
p cnf 2 4
1 2 0
1 -2 0
-1 2 0
-1 -2 0
```

DRAT

```
1 0
d 1 2 0
d 1 -2 0
2 0
d -1 2 0
0
```

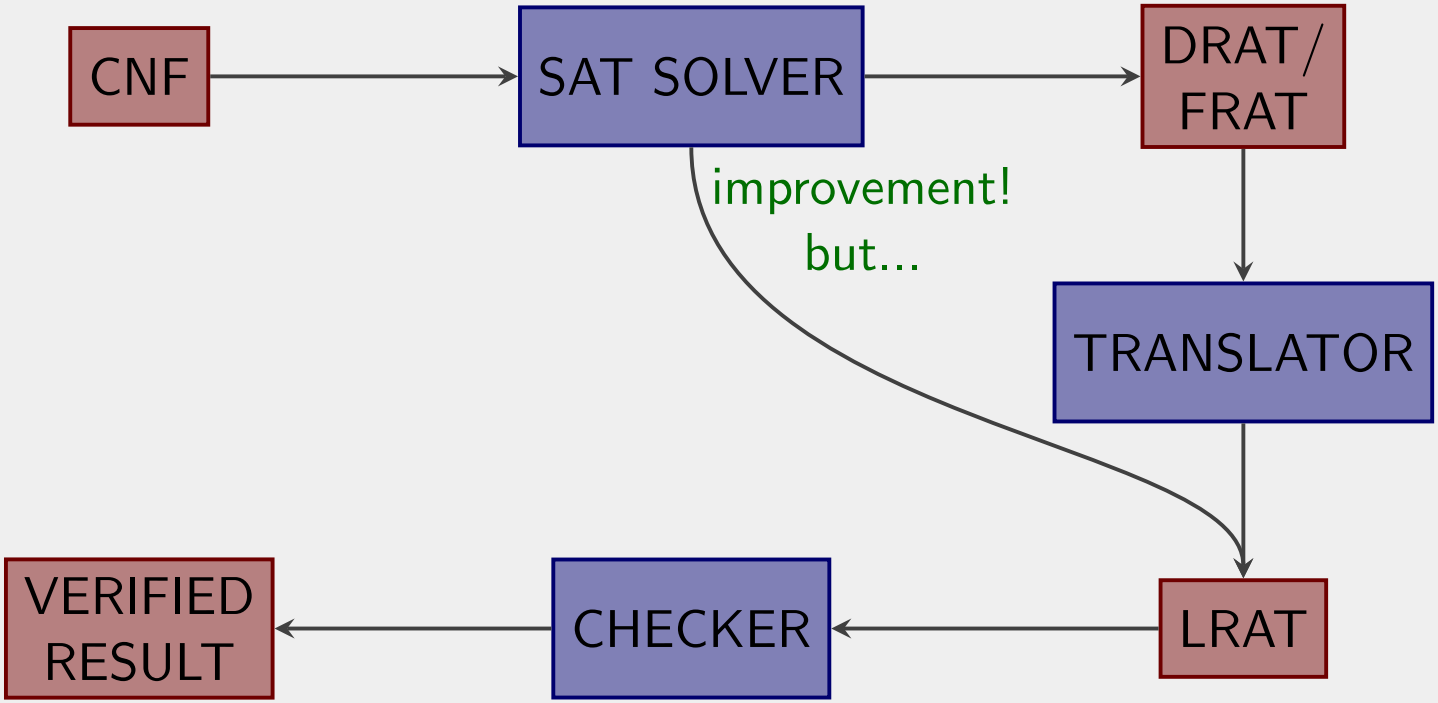
FRAT

```
o 1 1 2 0
o 2 1 -2 0
o 3 -1 2 0
o 4 -1 -2 0
a 5 1 0 l 1 2 0
d 1 1 2 0
d 2 1 -2 0
a 6 2 0
d 3 -1 2 0
a 7 0 l 5 6 4 0
f 4 -1 -2 0
f 5 1 0
f 6 2 0
f 7 0
```

LRAT

```
5 1 0 1 2 0
5 d 1 2 0
6 2 0 5 3 0
6 d 3 0
7 0 5 6 4 0
```

What are we doing again



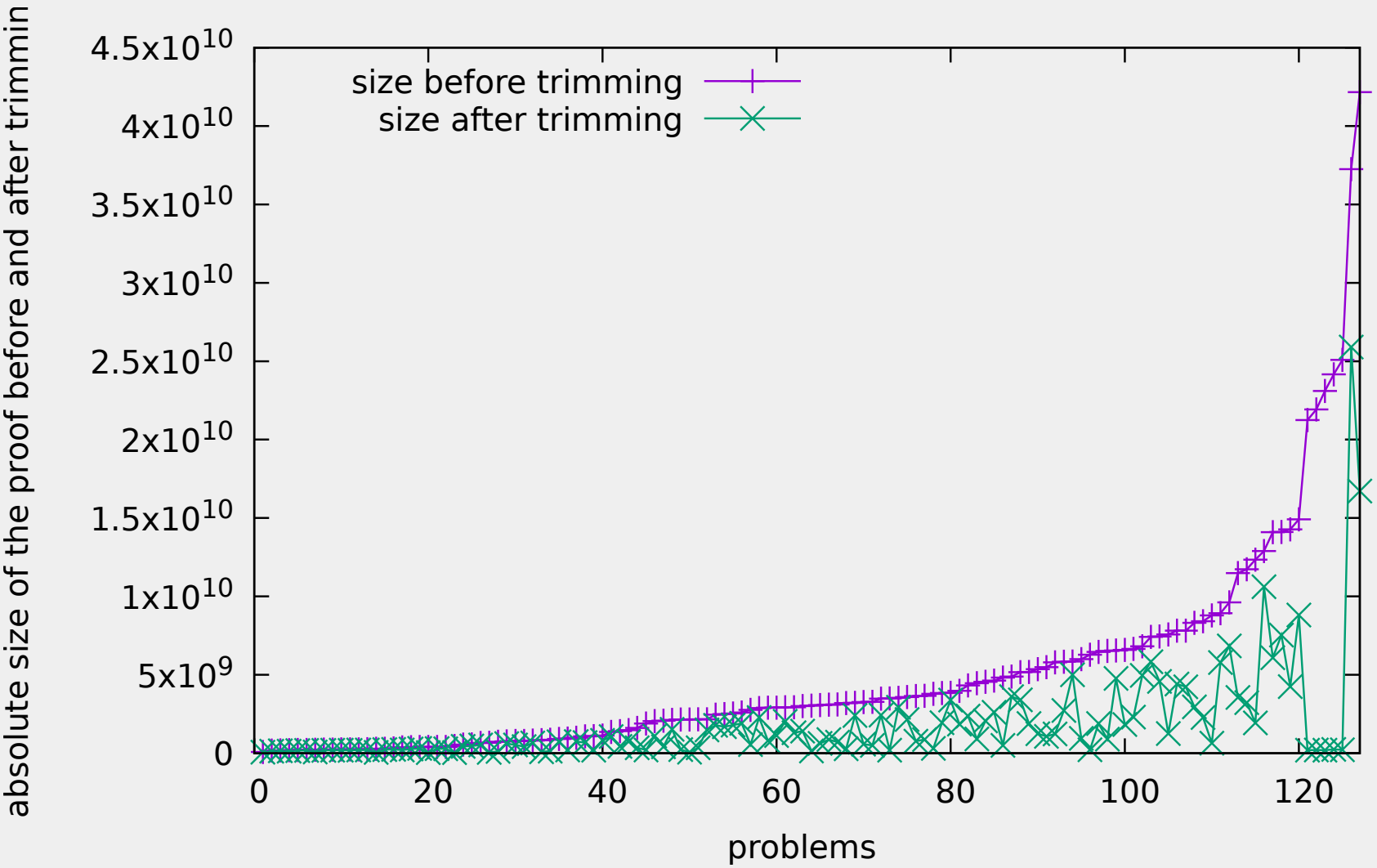
Implementation

- unit clauses
- order of traversal
- additional information

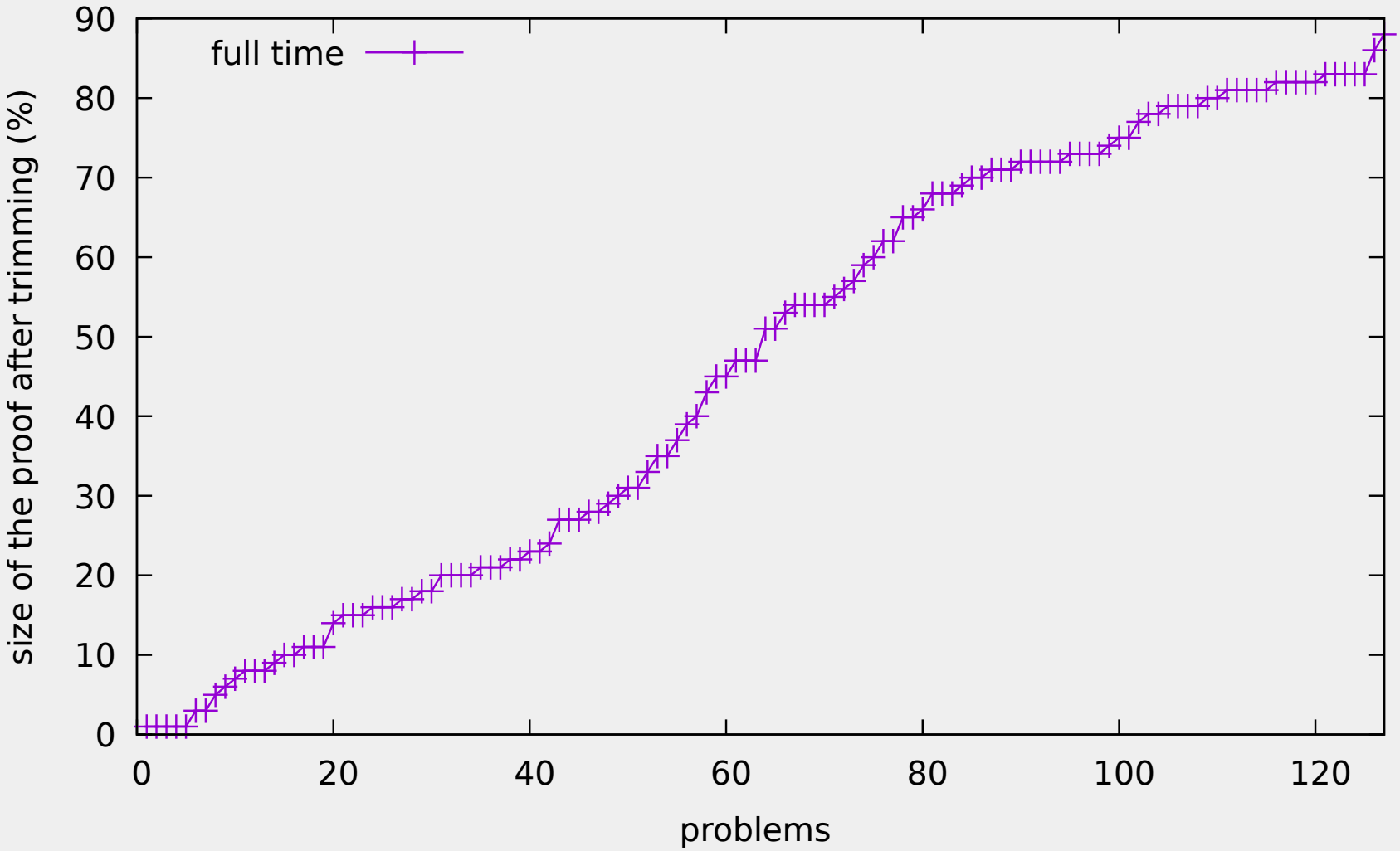
Experiments

- impact of trimming
- toolchain
- proof checking comparison

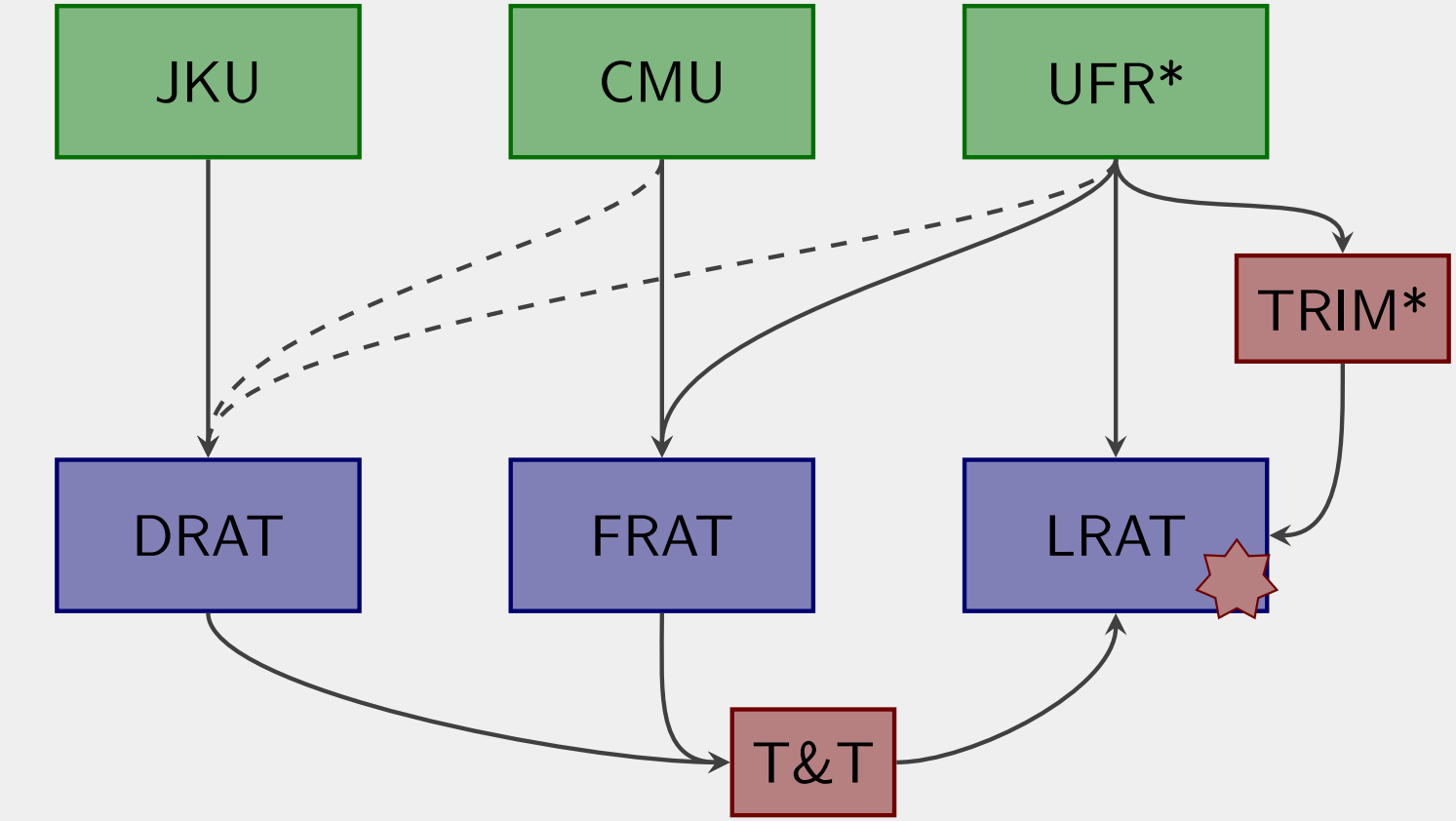
Proof trimming

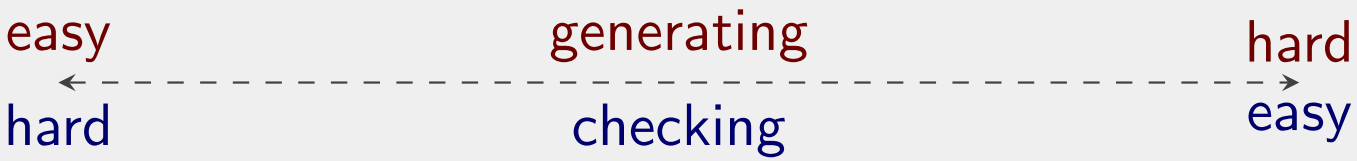


Proof trimming

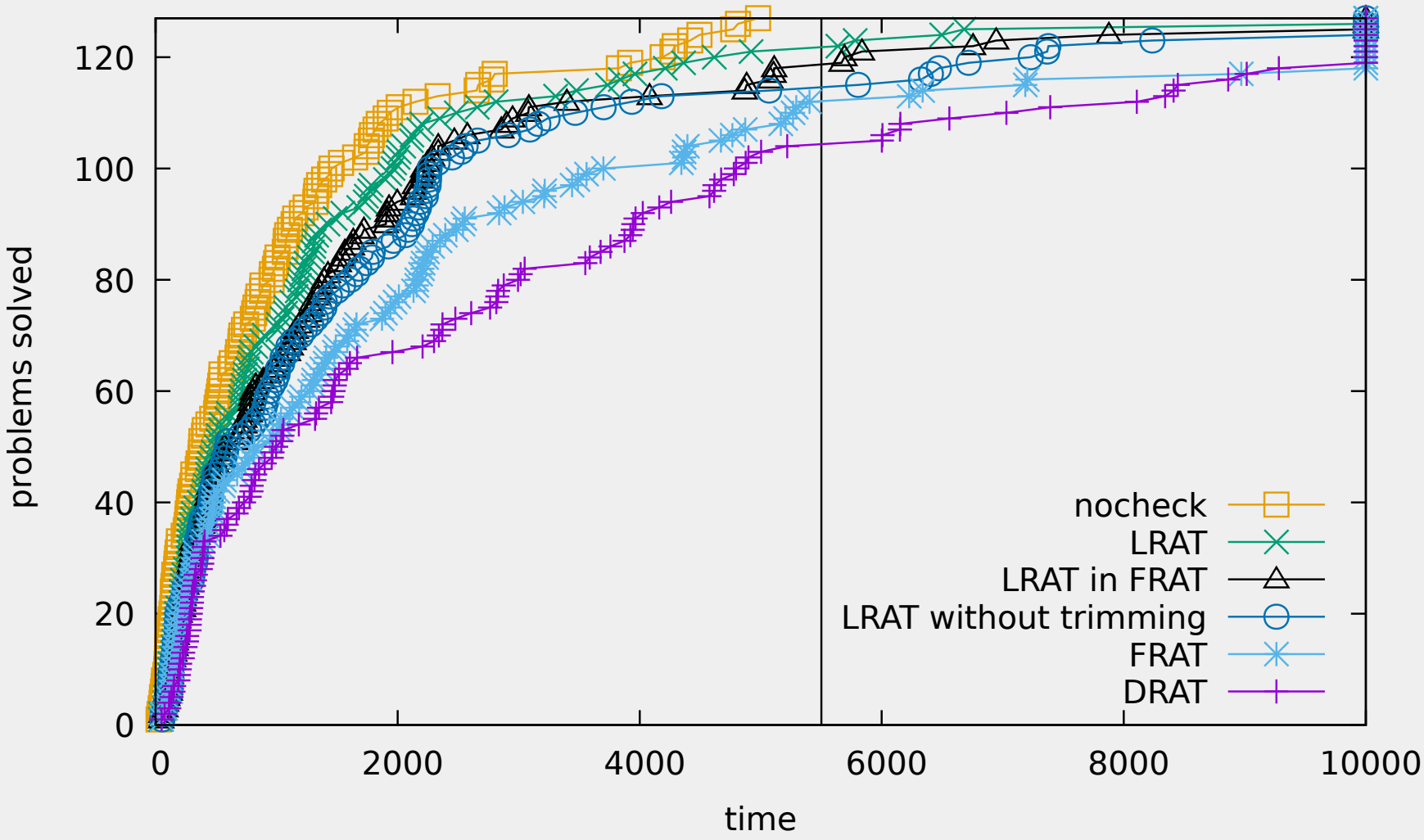


Toolchain

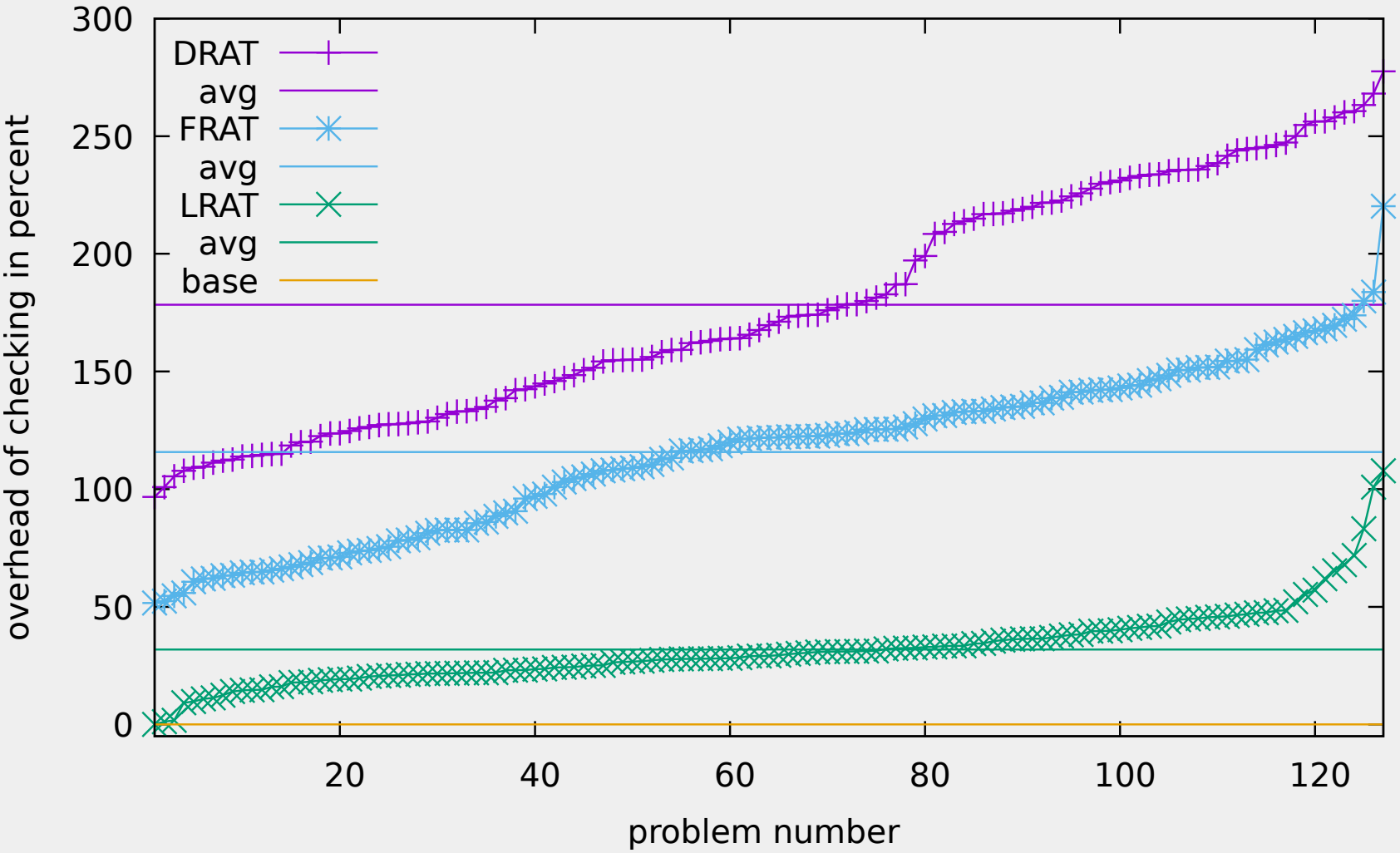

JKU
CMU
UFR*
TRIM*
DRAT
FRAT
LRAT
T&T


easy
generating
hard
hard
checking
easy

DRAT/FRAT/LRAT



Proof Checking Overhead



THANK YOU FOR LISTENING!

References

[BCH22] Seulkee Baek, Mario Carneiro, and Marijn J. H. Heule. “A Flexible Proof Format for SAT Solver-Elaborator Communication”. In: *Log. Methods Comput. Sci.* 18.2 (2022). DOI: 10.46298/lmcs-18(2:3)2022.

[Heu16] Marijn J. H. Heule. “The DRAT format and DRAT-trim checker”. In: *CoRR* abs/1610.06229 (2016). arXiv: 1610.06229. URL: http://arxiv.org/abs/1610.06229.

[KL15] Boris Konev and Alexei Lisitsa. “Computer-aided proof of Erdős discrepancy properties”. In: *Artif. Intell.* 224 (2015), pp. 103–118. DOI: 10.1016/j.artint.2015.03.004.

References

[Bie+99] Armin Biere et al. “Verifiying Safety Properties of a Power PC Microprocessor Using Symbolic Model Checking without BDDs”. In: *Proceedings of the 11th International Conference on Computer Aided Verification*. CAV ’99. Berlin, Heidelberg: Springer-Verlag, 1999, pp. 60–71. ISBN: 3540662022.

[Cru+17] Luís Cruz-Filipe et al. “Efficient Certified RAT Verification”. In: *Automated Deduction – CADE 26*. Ed. by Leonardo de Moura. Cham: Springer International Publishing, 2017, pp. 220–236. ISBN: 978-3-319-63046-5.