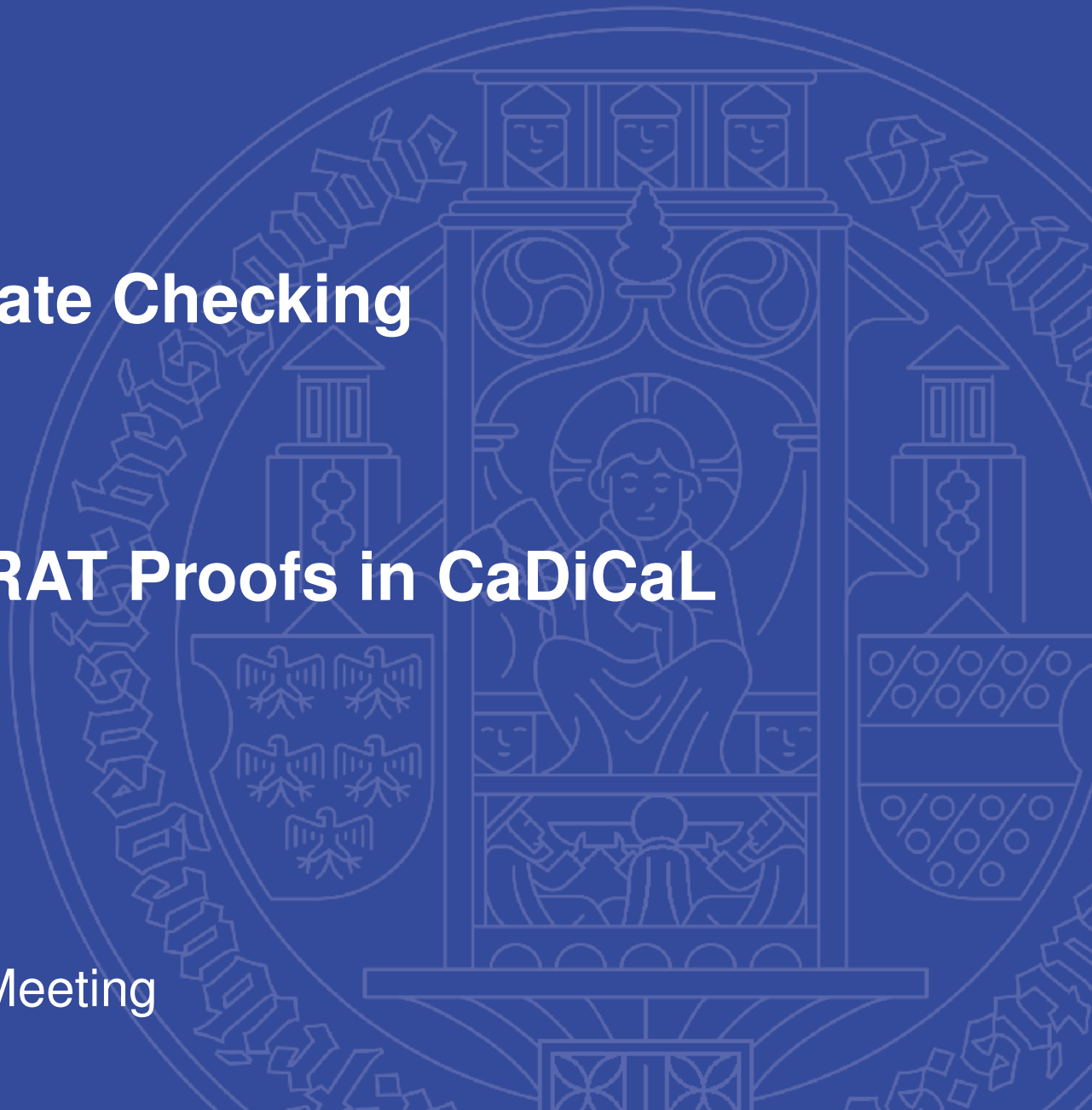
universität freiburg



Efficient Certificate Checking

Implementing LRAT Proofs in CaDiCaL

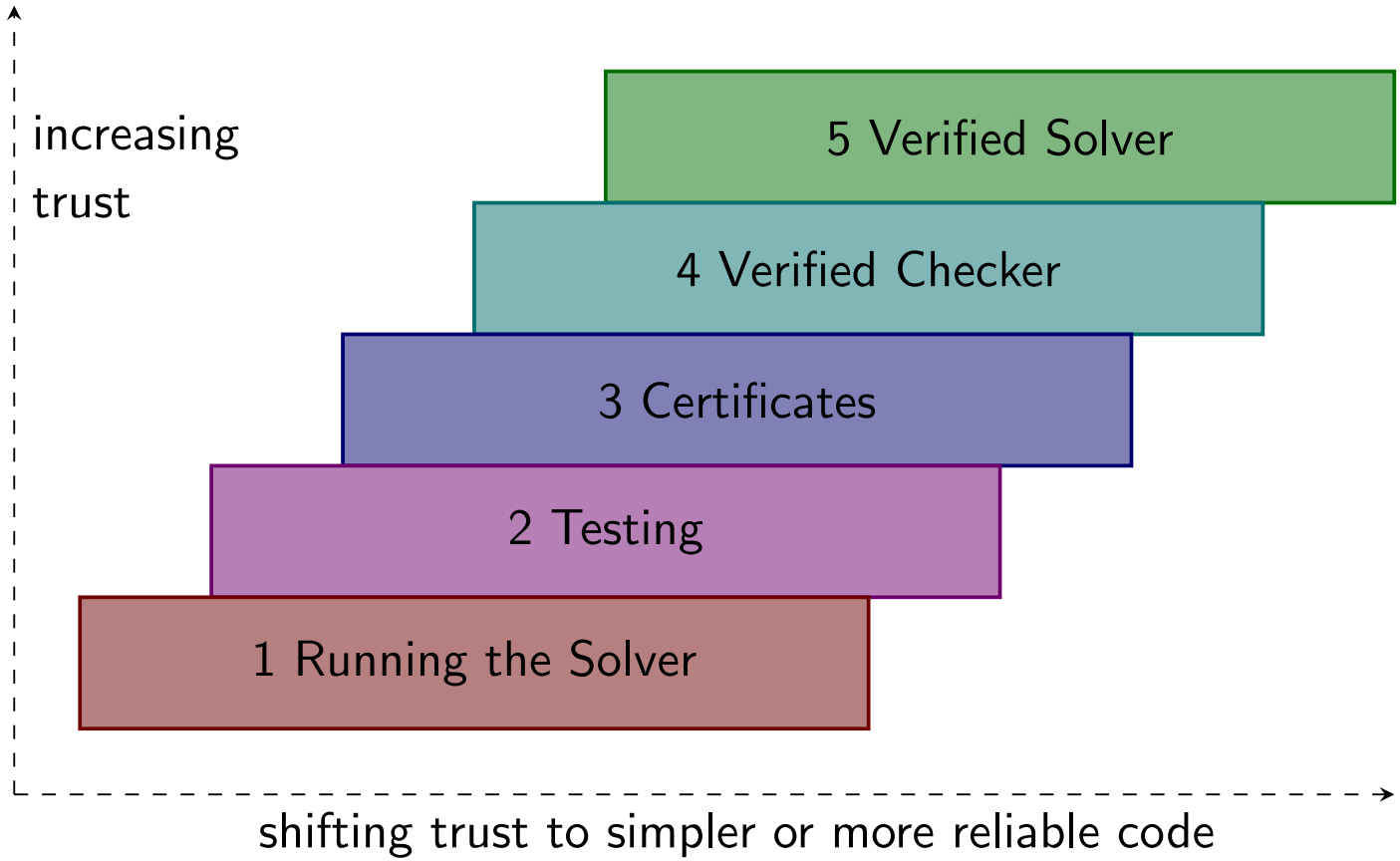
Florian Pollitt

15th Alpine Verification Meeting

SAT Solving

- pervasive
- correctness important
- machine checkable certificates
- industrial users like AWS, Systerel, etc.

Five Levels of Trust



Introducing Proof Formats

DIMACS

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

DRAT [Heu16]

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

LRAT [Cru+17]

```
1 0 1 2 0
2 0 1 -2 0
3 0 -1 2 0
4 0 -1 -2 0
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
```

LRAT in CaDiCaL

Proof Format	Proof size	Trimming tool	Trimmed size	Checking tool
DRAT	21GB	DRAT-TRIM	13GB	CAKE_LPR
LRAT	70GB	-	-	CAKE_LPR
LRAT	70GB	LRAT-TRIM	18GB	CAKE_LPR

	Solving time	Trimming time	Checking time	Total
no proof	4770s	-	-	4770s
DRAT	4801s	5639s	812s	11252s
LRAT	5100s	-	3819s	8919s
LRAT	5100s	263s	900s	6263s

Solving `sudoku-N30-10` on trust level four

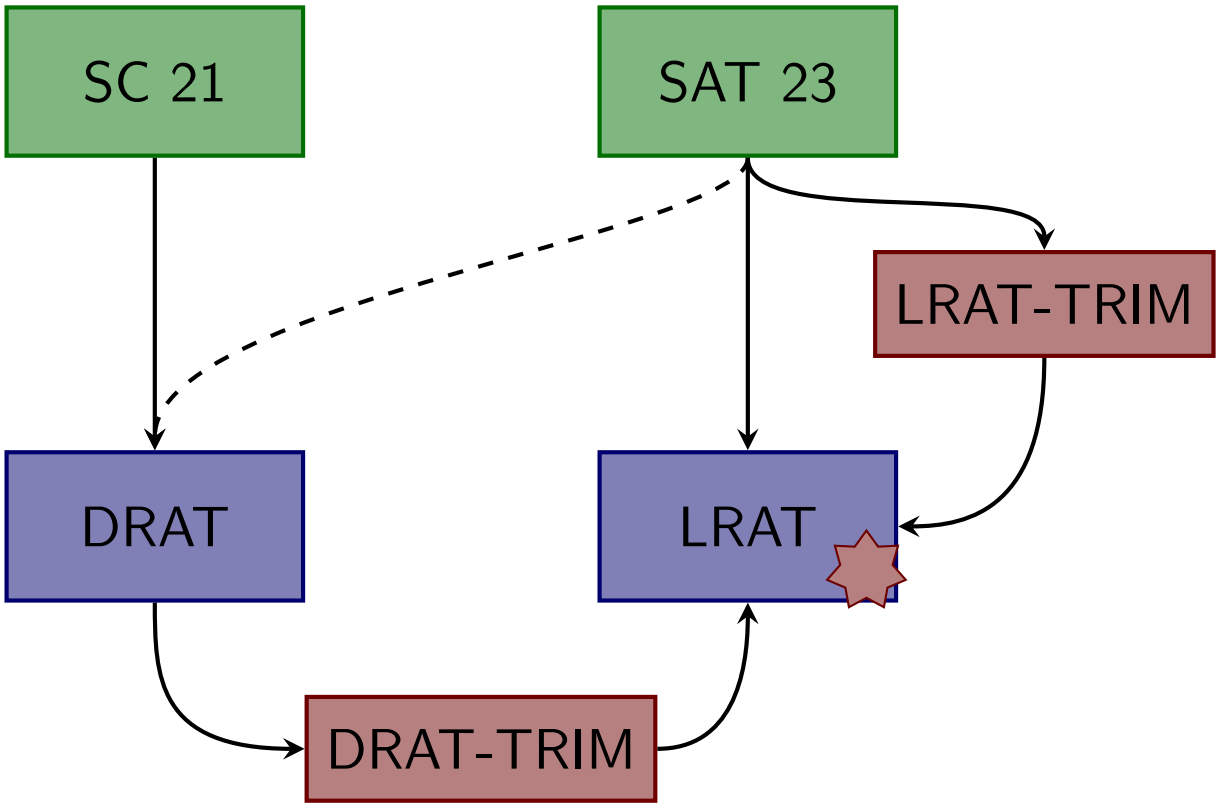
Comparing Proof Formats

DRAT [Heu16]	LRAT [Cru+17]	
×	✓	verified checker
✓	✓	unverified checker
×	✓	checker simplicity
×	✓	checker speed
✓	×	solver simplicity
✓	✓	solver speed
✓	×	proof size

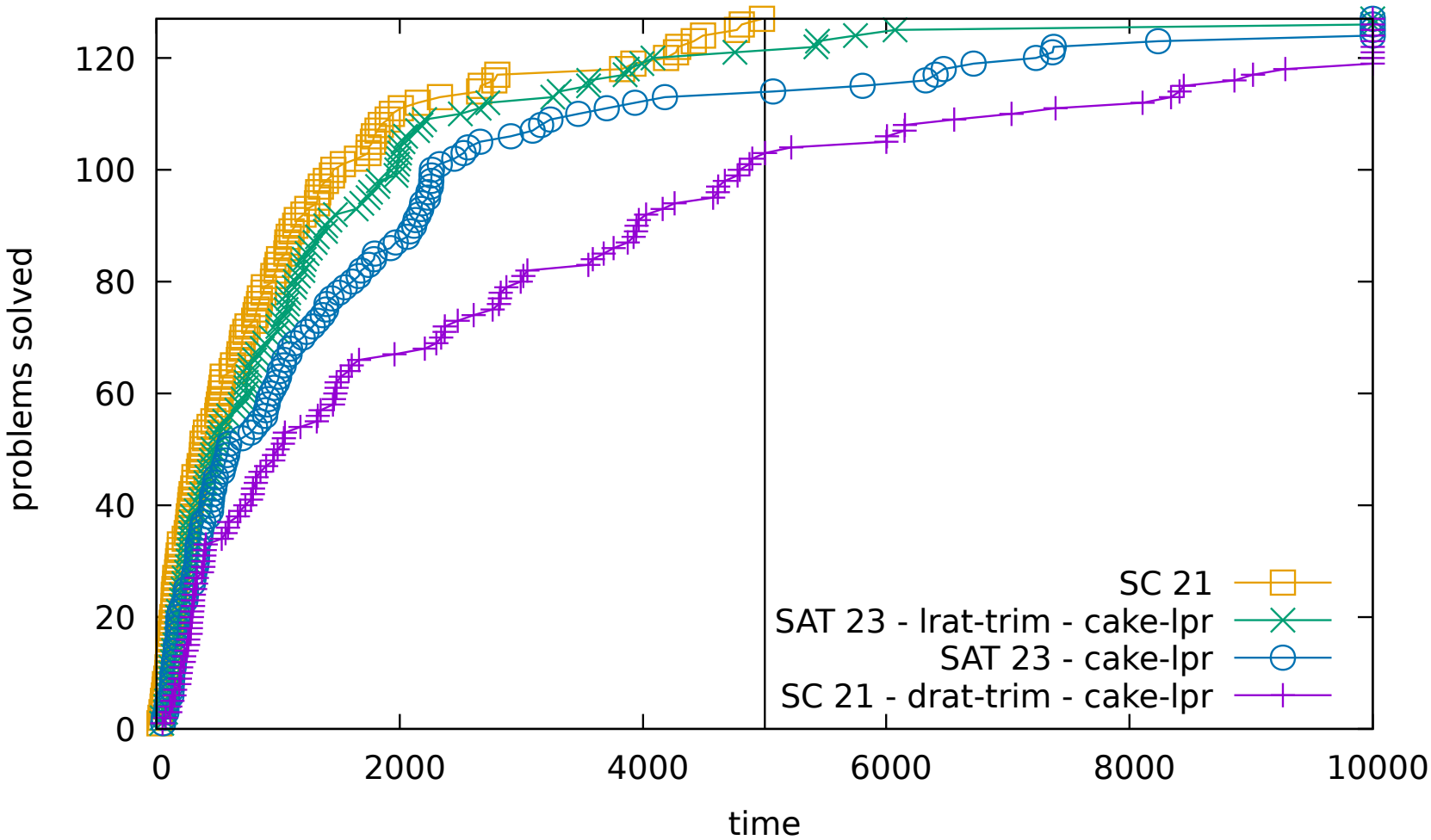
Implementation

- clause learning: analyze propagated clauses
- inprocessing: implicit propagation/resolution
- equivalent literal substitution: cycles/spanning trees

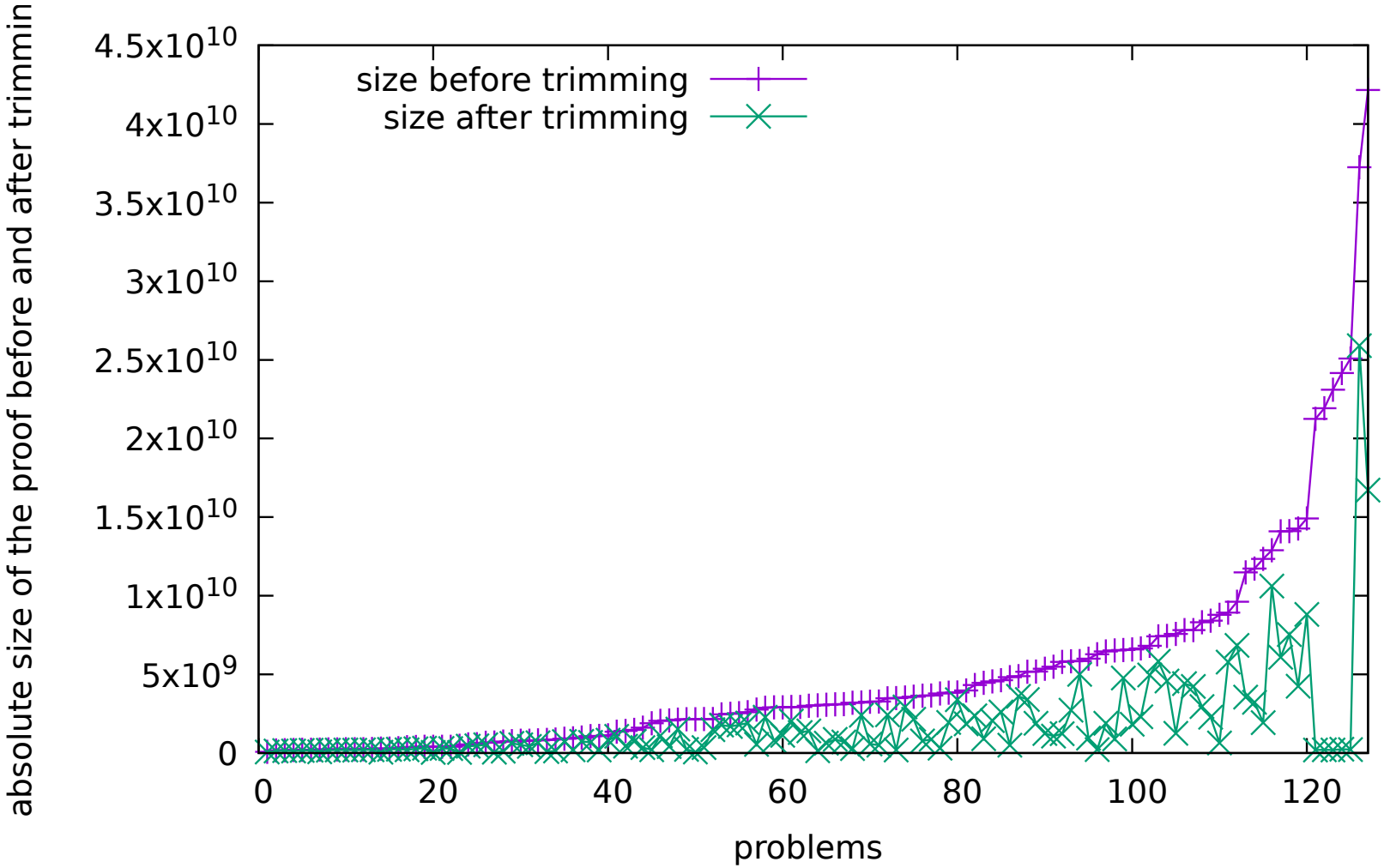
Experiments with CaDiCaL



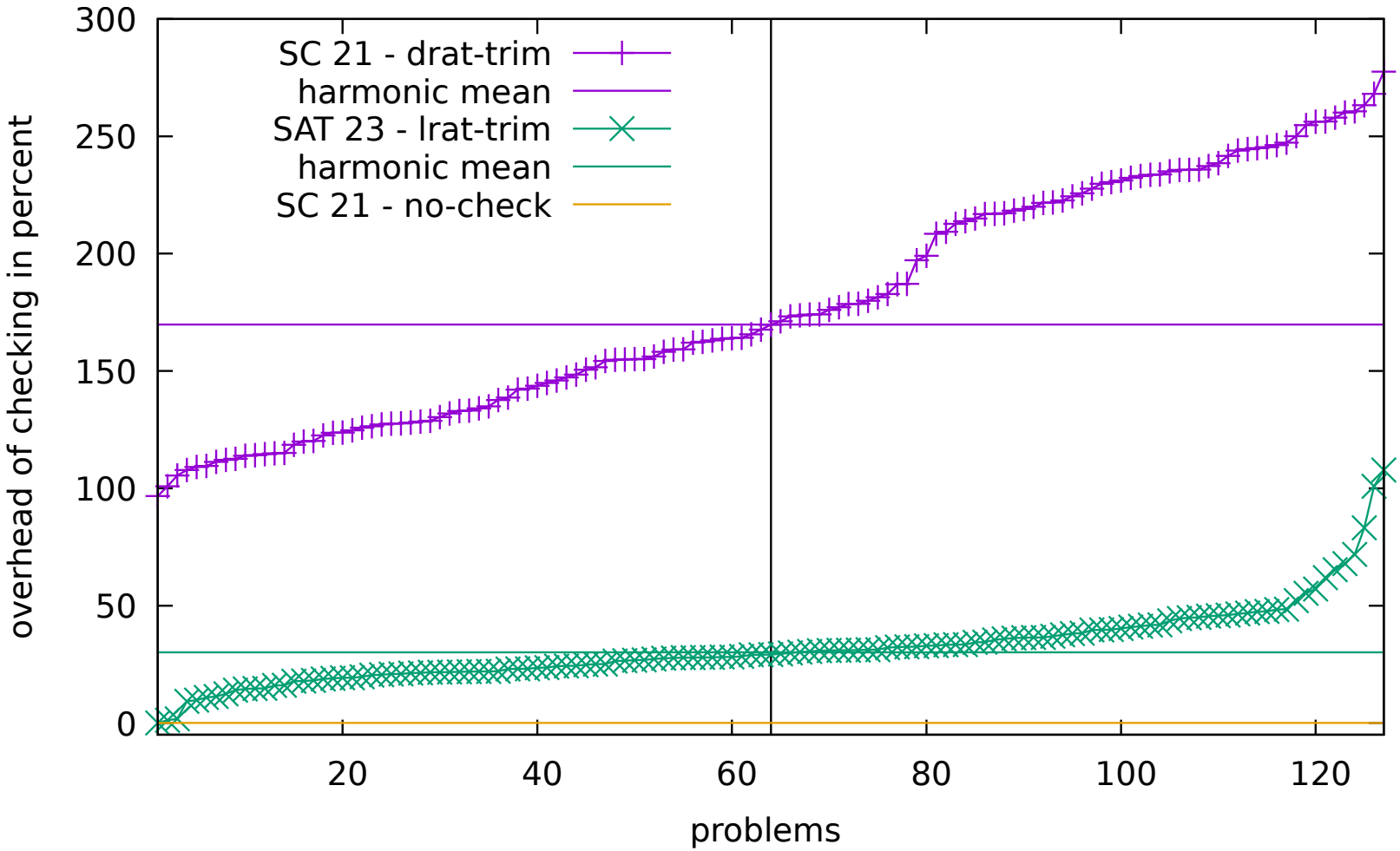
DRAT and LRAT



Proof Trimming



Proof Checking Overhead



Conclusion

- little overhead in solving
- big decrease in checking time
- faster checking then solving
- many interesting applications: interpolant building, other proof formats, ...
- future work: Combine trimming and checking, LRAT in more solvers, i.e., kissat or gimsatul

[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.

[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.