38 A Decision Procedure For Strong-Separation Logic

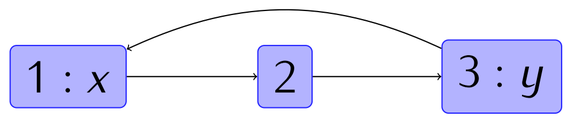
Author: Tomáš Dacík
Supervisor: prof. Ing. Tomáš Vojnar, Ph.D.

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2022

Separation Logic

- Separation logic (SL) is one of the most successful tools for verification of heap-manipulating programs
- Strong-separation logic (SSL) [1] is its recently introduced variant that improves decidability results
- This work is the first implementation of a decision procedure for SSL

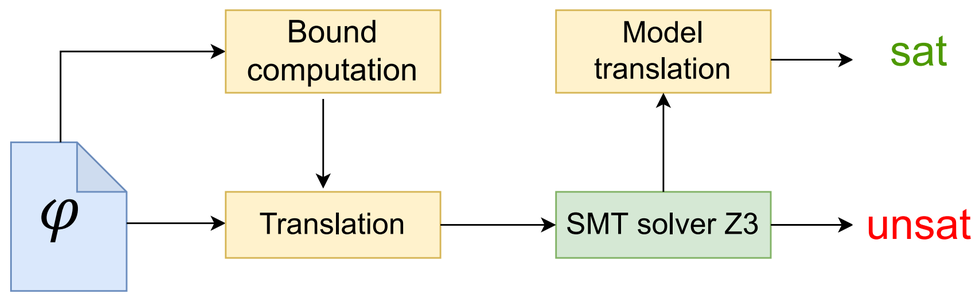


$$\models \quad \mathsf{ls}(x, y) * y \mapsto x$$

A heap contains a list-segment between x and y *and separately* a pointer from y to x.

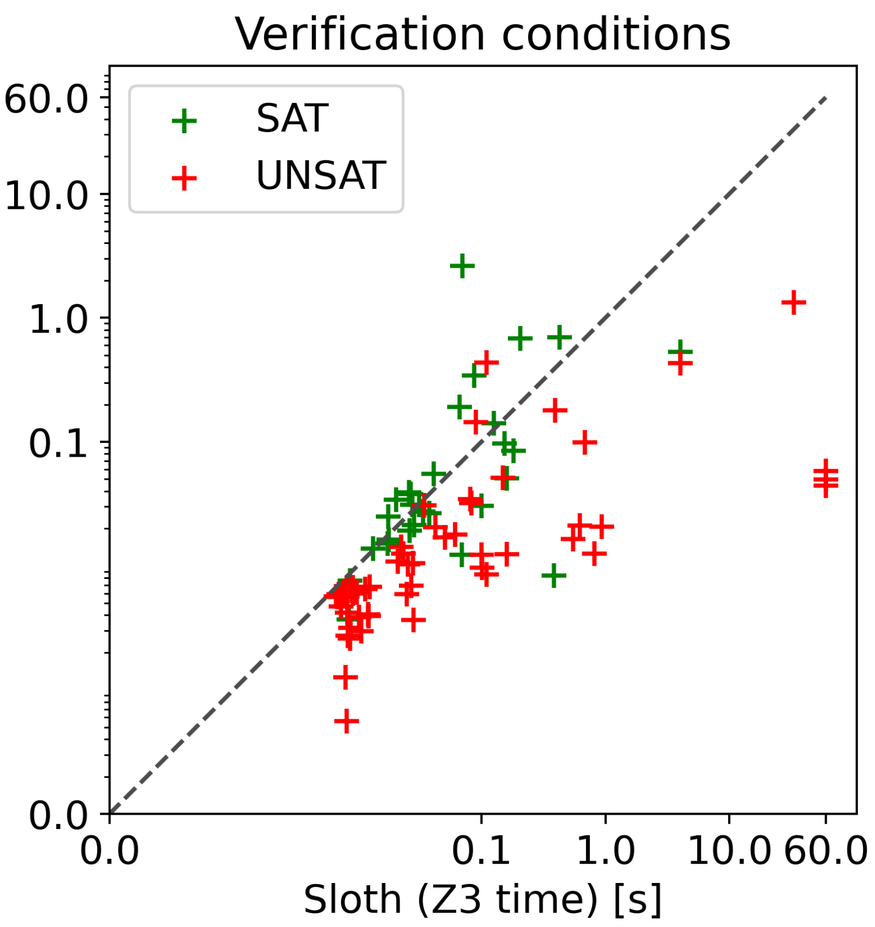
Proposed Decision Procedure

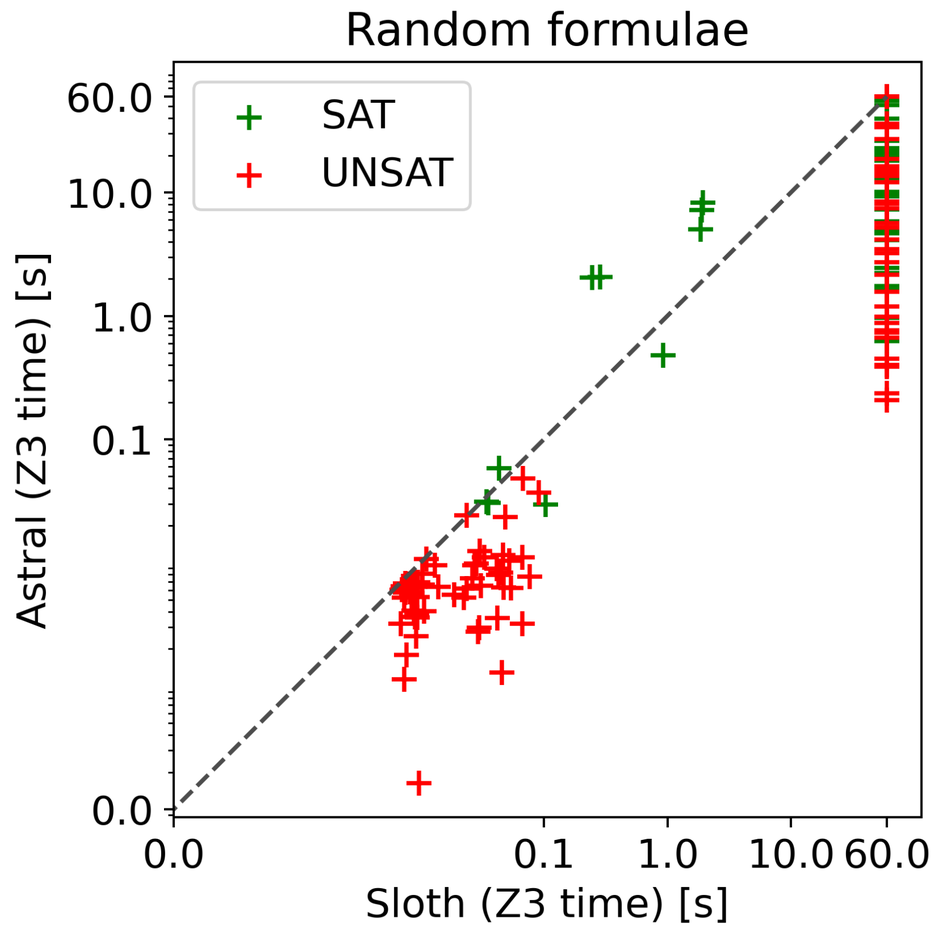
- Based on a translation to first-order logic, currently with the Microsoft's Z3 solver as the backend
- Improved computation of bounds on the number of memory locations in model and list segment lengths in a model



Experimental Evaluation

- Our decision procedure is implemented in a new tool called Astral
- Experiments on benchmarks from the international competition of solvers for separation logic SL-COMP (both on real-life verification problems and random formulae in a fragment where SL and SSL coincides)
- A comparison with a translation-based decision procedure for SL implemented in the tool Sloth [2]





References

[1] Jens Pagel and Florian Zuleger. Strong-separation logic. *ACM Trans. Program. Lang. Syst.*, nov 2021.

[2] Jens Katelaan, Dejan Jovanovic, and Georg Weissenbacher. A Separation Logic with Data: Small Models and Automation. In *IJCAR*, 2018.

The work was supported by the H2020 ECSEL project Arrowhead Tools.