SEAL: Symbolic Execution with Separation Logic

Tomáš Brablec[1] Tomáš Dacík[1] Tomáš Vojnar[1,2]

[1] Brno University of Technology

[2] Masaryk University

Seal

- Seal is a shape analyser with separation logic as the abstract domain
  - using the Astral[1] solver to check formulae in SL
  - Modular – verification and reasoning in SL are separated
  - Astral is based on translation to SMT, which allows combination with other theories (Seal currently supports only simple integer properties)

- Existing program analysers based on SL (Infer, PredatorHP, Broom, ...) use custom machinery to deal with SL formulae:
  - Often incomplete
  - Often deeply tied to verification procedure $\rightsquigarrow$ hard to extend
  - Often limited support for reasoning over data stored in data structures

[1] T. Dacík, A. Rogalewicz, T. Vojnar, and F. Zuleger. Deciding Boolean Separation Logic via Small Models. In TACAS 2024.

SEAL: Verification Approach

- Forward shape analysis with abstraction based on inductive predicates
- currently only a fixed set of list predicates
  - singly-linked lists, doubly-linked lists, nested singly-linked lists
- we plan to extend the tool to infer custom inductive predicates during analysis
- Implemented as a plugin of the Frama-C platform
  - Currently stand-alone, we would like to integrate it as a new abstract domain in Frama-C's abstract interpreter EVA

Seal: LinkedLists subcategory of SV-COMP'26

Analyser	Score	Correct true	Correct false
PredatorHP	220	96	28
CPAchecker	208	90	28
symbiotic	130	51	28
CBMC	127	50	28
Seal	114	55	4
Bubaak	114	48	18
Mopsa	96	48	0
ESBMC	96	50	28
2LS	90	46	14
DIVINE	84	42	0
UAutomizer	22	10	2
UTaipan	14	6	2

Seal does not produce any incorrect verdicts

Seal: LinkedLists category of SV-COMP'26 II

- Results for the subset of LinkedLists with:
  - Correct programs only
  - Unbounded data structures
  - 55 programs in total

- No other analyser scored any points

Analyser	True	False	No res.	Time [s]
PredatorHP	46	14	9	77
CPAchecker	40	13	16	1550
Seal	14	2	53	166
2LS	3	13	53	92