Songbird: an Inductive Theorem Prover for Separation Logic Entailments

Quang-Trung Ta[†], Ton-Chanh Le[*], Thanh-Toan Nguyen[†], Siau-Cheng Khoo[†], Wei-Ngan Chin[†]

[†]National University of Singapore, Singapore
[*]Stevens Institute of Technology, USA

1 Description

Songbird is an automated theorem prover for separation logic entailments. It is initally developed as a research tool at the National University of Singapore. The detailed information of Songbird is as follows:

Team members

- Quang-Trung Ta, National University of Singapore, Singapore
- Ton-Chanh Le, Stevens Institute of Technology, USA
- Thanh-Toan Nguyen, National University of Singapore, Singapore
- Siau-Cheng Khoo, National University of Singapore, Singapore
- Wei-Ngan Chin, National University of Singapore, Singapore

Separation logic fragment. We target to prove entailments in the fragment of symbolic-heap separation logic with inductive definitions and linear arithmetics. Detailed background of this logic fragment can be referred to in the following works [1, 4, 3].

Underlying theory. Songbird employs mathematical induction to prove entailments involving user-defined inductive heap predicates. In addition, Songbird is also equipped with powerful proof techniques to assist in proving the entailments. These include a mutual induction proof system [4] and a lemma synthesis framework [3].

Solver architecture. Songbird is implemented using the OCaml programming language. It utilizes the solver Z3 [2] as the underlying SMT solver for the first-order logic formula which contains equality and linear arithmetic constraints. The input syntax of Songbird is described at: https://songbird-prover.github.io/lemma-synthesis/index.html.

Strength and weakness. Songbird can efficiently prove separation logic entailments, especially the ones contain inductive heap predicates and linear arithmetic constraints. Songbird particiapted in the separation logic competition SL-COMP 2018, and won the best result for 4 (over 9) competition divisions: qf_shid_entl, qf_shidlia_entl, shid_entl, shidlia_entl. It can also solve 100%

problems of other 2 divisions: qf_shls_entl, qf_shls_sat, although the runtime is slower than the best prover of these divisions.

Contact. The corresponding author of Songbird is: Dr. Quang-Trung Ta, National University of Singapore. Email: taqt@comp.nus.edu.sg.

Project page. For more information, please refer to this website: https://songbird-prover.github.io/.

References

[1] Josh Berdine, Cristiano Calcagno, and Peter W. O'Hearn. "Symbolic Execution with Separation Logic". In: *Asian Symposium on Programming Languages and Systems (APLAS)*. 2005, pp. 52–68.

[2] Leonardo Mendonça De Moura and Nikolaj Bjørner. "Z3: An Efficient SMT Solver". In: *Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS)*. 2008, pp. 337–340.

[3] Quang-Trung Ta, Ton Chanh Le, Siau-Cheng Khoo, and Wei-Ngan Chin. "Automated Lemma Synthesis in Symbolic-Heap Separation Logic". In: *Symposium on Principles of Programming Languages (POPL)*. 2018, 9:1–9:29.

[4] Quang-Trung Ta, Ton Chanh Le, Siau-Cheng Khoo, and Wei-Ngan Chin. "Automated Mutual Explicit Induction Proof in Separation Logic". In: *Symposium on Formal Methods (FM)*. 2016, pp. 659–676.