David, Cristina; **Kroening, Daniel**; **Lewis, Matt**

Propositional reasoning about safety and termination of heap-manipulating programs. (English) Zbl 1335.68051

Vitek, Jan (ed.), Programming languages and systems. 24th European symposium on programming, ESOP 2015, held as part of the European joint conferences on theory and practice of software, ETAPS 2015, London, UK, April 11–18, 2015. Proceedings. Berlin: Springer (ISBN 978-3-662-46668-1/pbk; 978-3-662-46669-8/ebook). Lecture Notes in Computer Science 9032, 661-684 (2015).

Summary: This paper shows that it is possible to reason about the safety and termination of programs handling potentially cyclic, singly-linked lists using propositional reasoning even when the safety invariants and termination arguments depend on constraints over the lengths of lists. For this purpose, we propose the theory SLH of singly-linked lists with length, which is able to capture non-trivial interactions between shape and arithmetic. When using the theory of bit-vector arithmetic as background theory, SLH is efficiently decidable via a reduction to SAT. We show the utility of SLH for software verification by using it to express safety invariants and termination arguments for programs manipulating potentially cyclic, singly-linked lists with unrestricted, unspecified sharing. We also provide an implementation of the decision procedure and apply it to check safety and termination proofs for several heap-manipulating programs.

For the entire collection see [Zbl 1333.68020].

MSC:

68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)

Keywords:

heap; SAT; safety; termination

Software:

THOR

Full Text: DOI