

Berdine, Josh; Calcagno, Cristiano; Cook, Byron; Distefano, Dino; O’Hearn, Peter W.; Wies, Thomas; Yang, Hongseok

Shape analysis for composite data structures. (English) [Zbl 1135.68372](#)

Damm, Werner (ed.) et al., Computer aided verification. 19th international conference, CAV 2007, Berlin, Germany, July 3–7, 2007. Proceedings. Berlin: Springer (ISBN 978-3-540-73367-6/pbk). Lecture Notes in Computer Science 4590, 178-192 (2007).

Summary: We propose a shape analysis that adapts to some of the complex composite data structures found in industrial systems-level programs. Examples of such data structures include “cyclic doubly-linked lists of acyclic singly-linked lists”, “singly-linked lists of cyclic doubly-linked lists with back-pointers to head nodes”, etc. The analysis introduces the use of generic higher-order inductive predicates describing spatial relationships together with a method of synthesizing new parameterized spatial predicates which can be used in combination with the higher-order predicates. In order to evaluate the proposed approach for realistic programs we have performed experiments on examples drawn from device drivers: the analysis proved safety of the data structure manipulation of several routines belonging to an IEEE 1394 (firewire) driver, and also found several previously unknown memory safety bugs.

For the entire collection see [\[Zbl 1119.68005\]](#).

MSC:

[68P05](#) Data structures

Cited in **13** Documents

Software:

[TVLA](#)

Full Text: [DOI](#)