Farinier, Benjamin; **David, Robin**; **Bardin, Sébastien**; **Lemerre, Matthieu**

Arrays made simpler: an efficient, scalable and thorough preprocessing. (English)

Zbl 1415.68145

Barthe, Gilles (ed.) et al., LPAR-22. 22nd international conference on logic for programming, artificial intelligence and reasoning, Awassa, Ethiopia, November 17–21, 2018. Selected papers. Manchester: EasyChair. EPiC Ser. Comput. 57, 363-380 (2018).

Summary: The theory of arrays has a central place in software verification due to its ability to model memory or data structures. Yet, this theory is known to be hard to solve in both theory and practice, especially in the case of very long formulas coming from unrolling-based verification methods. Standard simplification techniques à la read-over-write suffer from two main drawbacks: they do not scale on very long sequences of stores and they miss many simplification opportunities because of a crude syntactic (dis-)equality reasoning. We propose a new approach to array formula simplification based on a new dedicated data structure together with original simplifications and low-cost reasoning. The technique is efficient, scalable and it yields significant simplification. The impact on formula resolution is always positive, and it can be dramatic on some specific classes of problems of interest, e.g., very long formula or binary-level symbolic execution. While currently implemented as a preprocessing, the approach would benefit from a deeper integration in an array solver.

For the entire collection see [Zbl 1407.68021].

MSC:

68Q60 Specification and verification (program logics, model checking, etc.)
68P05 Data structures

Keywords:

read-over-write simplification; satisfiability modulo theory; theory of arrays

Software:

BINSEC/SE; z3

Full Text: DOI