zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Asadi, Sepideh; **Blicha, Martin**; **Fedyukovich, Grigory**; **Hyvärinen, Antti**; **Even-Mendoza, Karine**; **Sharygina, Natasha**; **Chockler, Hana**

Function summarization modulo theories. (English) Zbl 1415.68141

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, 56-75 (2018).

Summary: SMT-based program verification can achieve high precision using bit-precise models or combinations of different theories. Often such approaches suffer from problems related to scalability due to the complexity of the underlying decision procedures. Precision is traded for performance by increasing the abstraction level of the model. As the level of abstraction increases, missing important details of the program model becomes problematic. In this paper, we address this problem with an incremental verification approach that alternates precision of the program modules on demand. The idea is to model a program using the lightest possible (i.e., less expensive) theories that suffice to verify the desired property. To this end, we employ safe over-approximations for the program based on both function summaries and light-weight SMT theories. If during verification it turns out that the precision is too low, our approach lazily strengthens all affected summaries or the theory through an iterative refinement procedure. The resulting summarization framework provides a natural and light-weight approach for carrying information between different theories. An experimental evaluation with a bounded model checker for C on a wide range of benchmarks demonstrates that our approach scales well, often effortlessly solving instances where the state-of-the-art model checker CBMC runs out of time or memory.

For the entire collection see [Zbl 1407.68021].

MSC:

68Q60 Specification and verification (program logics, model checking, etc.)
68T20 Problem solving in the context of artificial intelligence (heuristics, search strategies, etc.)

Keywords:

bounded model checking; Craig interpolation; function summaries; incremental verification; satisfiability modulo theories; software verification

Full Text: DOI

© 2021 FIZ Karlsruhe GmbH