Iwayama, Naoki; Kobayashi, Naoki; Suzuki, Ryota; Tsukada, Takeshi
Predicate abstraction and CEGAR for $\nu$HFL$_{\mathbb{Z}}$ validity checking. (English) Zbl 1474.68190

Summary: We propose an automated method for $\nu$HFL$_{\mathbb{Z}}$ validity checking. HFL$_{\mathbb{Z}}$ is an extension of the higher-order fixpoint logic HFL with integers, and $\nu$HFL$_{\mathbb{Z}}$ is a restriction of it to the fragment without the least fixpoint operator. The validity checking problem for HFL$_{\mathbb{Z}}$ has recently been shown to provide a uniform approach to higher-order program verification. The restriction to $\nu$HFL$_{\mathbb{Z}}$ studied in this paper already provides an automated method for a large class of program verification problems including safety and non-termination verification, and also serves as a key building block for solving the validity checking problem for full HFL$_{\mathbb{Z}}$. Our approach is based on predicate abstraction and counterexample-guided abstraction refinement (CEGAR). We have implemented the proposed method, and applied it to program verification. According to experiments, our tool outperforms a closely related tool called Horus in terms of precision, and is competitive with a more specialized program verification tool called MoCHi despite the generality of our approach.

For the entire collection see [Zbl 1471.68022].

MSC:
68Q60 Specification and verification (program logics, model checking, etc.)
03B70 Logic in computer science
68N30 Mathematical aspects of software engineering (specification, verification, metrics, requirements, etc.)

Full Text: DOI

References: